BLOCKCHAIN
THROUGH A LEGAL LENS
Abstract
Blockchain technology is one of the most promising new technologies since the advent of the Internet. With blockchain’s decentralized, immutable, and anonymous features, it has the capability of changing the way we interact, how digital information is stored and retrieved, and who has access to such information. As companies of all sizes, along with a robust development community, are devoting substantial resources to blockchain applications, legal practitioners need to become acquainted with the technology. Practitioners not only need to understand how blockchain technology may be governed by existing laws and regulations, but also be participants in the creation of, and advocacy for, new laws and regulations that protect individuals while also encouraging innovation in the blockchain ecosystem.

As is common with emerging technologies, blockchain development is far outpacing efforts by regulators and courts to address the myriad of unique issues that the technology raises. Blockchain Through A Legal Lens provides a comprehensive overview of current federal, state, and select international laws governing blockchain technology. Where laws or regulations do not exist, or potentially relevant laws or regulations have not yet been applied, the treatise aims to provide thoughtful analysis of how the existing U.S. legal framework and jurisprudence may apply to the intersection of blockchain technology and a variety of practice areas, such as intellectual property, anti-money laundering, consumer protection, property, and contracts.
Contributing Authors

Lee Weiss, Blockchains General Counsel
Stephanie Sciarani, Blockchains Deputy General Counsel
Emily Friedman
Albert Lum

Editors

Lee Weiss, Blockchains General Counsel
Stephanie Sciarani, Blockchains Deputy General Counsel
Andrew Wilmar
Eric Berlin

Acknowledgements

Nicole Emmerich, Blockchains Marketing Specialist
Elaina Duffy, Blockchains Marketing Director
Richard Escalante, Blockchains Digital Media Director
Disclaimer

Blockchain Through A Legal Lens is a work in progress. Since blockchain technology and the law change rapidly, there may be portions of the treatise that are not current. In order to provide the reader with the most up-to-date information, the treatise will be updated on a regular basis. However, it is advised that you conduct your own research, including whether the statements of law contained in the treatise are applicable to the jurisdiction in which you are practicing or conducting business. It is important that prior to relying upon, or using, such information you verify the information is still accurate as laws may have been amended or overturned by subsequent case law or legislation since the treatise was published.

The content in Blockchain Through A Legal Lens is provided for informational purposes only. None of the content is intended to be, and does not, constitute legal advice, or any other advice. All of the content is general in nature and not specific to your circumstances. You should not rely on the treatise to make any legal decisions. It is recommended that you retain an attorney for all legal advice and issues. Nothing in the treatise forms an attorney-client relationship between you and the authors, editors, or contributors. Blockchains, the authors, editors, and contributors do not accept responsibility for any loss or inconvenience caused by your reliance on any material contained in this treatise.
# Table of Contents

**Chapter 1: The History of Virtual Currency** ................................................................. 1

1.1 Precursors to Decentralized Virtual Currencies ....................................................... 1

1.1.1 E-Cash ............................................................................................................... 2
1.1.2 E-Gold .............................................................................................................. 3
1.1.3 B-Money .......................................................................................................... 4
1.1.4 WebMoney ........................................................................................................ 4
1.1.5 Linden Dollars ................................................................................................... 5
1.1.6 Bit Gold and Reusable Proof-of-Work ............................................................... 5
1.1.7 Liberty Reserve ................................................................................................ 6
1.1.8 M-Pesa ............................................................................................................ 7
1.1.9 SUCRE ............................................................................................................ 8

1.2 Decentralized Virtual Currencies ............................................................................. 8

1.2.1 Bitcoin ............................................................................................................ 8
1.2.2 Ethereum ......................................................................................................... 9
1.2.3 Dash ................................................................................................................ 10
1.2.4 Ripple ............................................................................................................. 11

**Chapter 2: Blockchain Technology** ......................................................................... 12

2.1 Public Key Cryptography ......................................................................................... 12

2.1.1 Encryption ....................................................................................................... 12
2.1.2 Digital Signatures ............................................................................................ 12

2.2 Blockchain ............................................................................................................. 13

2.2.1 Blockchain as a Ledger of Transactions ............................................................ 13
2.2.2 The Mining Process and Verification of Transactions ....................................... 15

2.2.2.1 Peer-to-Peer Network ................................................................................... 16
2.2.2.2 Proof-of-Work ............................................................................................. 17
2.2.2.3 Proof-of-Stake ............................................................................................. 18
2.2.2.4 Cloud Mining ............................................................................................... 20

2.2.3 GHOST and Uncles ......................................................................................... 20

2.3 Tokens .................................................................................................................. 21

2.4 Wallets .................................................................................................................. 22

2.5 Transaction Fees ................................................................................................... 23

2.5.1 The Bitcoin Network ......................................................................................... 23
2.5.2 The Ethereum Network .................................................................................... 24

2.6 Exchanges ............................................................................................................ 25

2.6.1 Centralized Exchanges ..................................................................................... 25
2.6.2 Decentralized Exchanges ................................................................................ 26

2.7 Virtual Currency ATMs ......................................................................................... 27

2.8 Executable Distributed Code Contracts ................................................................. 28

2.9 Decentralized Applications ..................................................................................... 29

2.10 Decentralized Autonomous Organizations ......................................................... 29
Chapter 3: Threats to Blockchain Networks

3.1 Cyberattacks

3.1.1 Social Engineering
3.1.2 Phising
3.1.3 Denial-of-Service
3.1.4 Distributed Denial-of-Service
3.1.5 Malware

3.1.5.1 Viruses, Trojan Horses and Worms
3.1.5.2 Botnet
3.1.5.3 Sybil Attack
3.1.5.4 Ransomware

3.1.6 Replay Attack
3.1.7 51% Attack
3.1.8 Variations on the 51% Attack

3.1.8.1 Goldfinger Attack
3.1.8.2 Feather Forking
3.1.8.3 Eclipse

3.1.9 Selfish Mining
3.1.10 Finney Attack

Chapter 4: Current Virtual Currency and Blockchain Regulations and Legislative Efforts in the United States

4.1 Congressional Action Regarding Blockchain Technology and Virtual Currency

4.1.1 H. Res. 835
4.1.2 Congressional Blockchain Caucus
4.1.4 H.R. 3364 – Countering America’s Adversaries Through Sanctions Act
4.1.5 Pending Federal Legislation

4.1.5.1 H.R. 4768 – National Strategy for Combating the Financing of Transnational Criminal Organizations Act
4.1.5.2 H.R. 5036 – Financial Technology Protection Act
4.1.5.3 H.R. 6913 – Blockchain Promotion Act of 2018
4.1.5.4 H. Res. 1102 – Expressing Support for Digital Currencies and Blockchain Technology
4.1.5.5 H.R. 6974 – The Blockchain Regulatory Certainty Act
4.1.5.6 H.R. 6973 – The Safe Harbor for Taxpayers with Forked Assets Act of 2018

4.1.6 Other Congressional Initiatives That May Ultimately Impact Blockchain Technology and Cryptocurrency

4.1.6.1 Congressional FinTech and Payments Caucus
4.1.6.2 2018 Congressional Economic Report
4.1.6.3 Other Congressional Caucuses Related to New Technologies

4.2 State Legislation Regarding Blockchain Technology and Virtual Currency

4.2.1 State Regulation Specifically for Virtual Currency Businesses

4.2.1.1 New York’s BitLicense
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.1.2 Challenges to BitLicense and the NYDFS’s Authority</td>
<td>57</td>
</tr>
<tr>
<td>4.2.2 State Laws for the Licensing of Money Transmitters and Money</td>
<td></td>
</tr>
<tr>
<td>Services Businesses</td>
<td>58</td>
</tr>
<tr>
<td>4.2.2.1 States Money Transmission Laws That Expressly Cover Virtual</td>
<td></td>
</tr>
<tr>
<td>Currency or Have Been Interpreted to Include Virtual Currency</td>
<td>59</td>
</tr>
<tr>
<td>4.2.2.2 State Money Transmission Laws That Expressly Exclude Virtual</td>
<td>60</td>
</tr>
<tr>
<td>Currency</td>
<td></td>
</tr>
<tr>
<td>4.2.2.3 State Money Transmission Laws That Are Silent on Virtual</td>
<td>60</td>
</tr>
<tr>
<td>Currency</td>
<td></td>
</tr>
<tr>
<td>4.2.2.4 Specific Requirements of State Money Transmission Laws</td>
<td>63</td>
</tr>
<tr>
<td>4.2.3 Other State Blockchain and Cryptocurrency Legislation</td>
<td>64</td>
</tr>
<tr>
<td>4.2.4 State Tax Treatment of Virtual Currency Transactions</td>
<td>68</td>
</tr>
<tr>
<td>4.2.4.1 Sales and Use Taxes</td>
<td>68</td>
</tr>
<tr>
<td>4.2.4.2 Other State Taxes</td>
<td>70</td>
</tr>
<tr>
<td>4.2.4.3 Bills to Study Blockchain Technology</td>
<td>70</td>
</tr>
<tr>
<td>4.2.5 Uniform Law Commission</td>
<td>71</td>
</tr>
<tr>
<td>Chapter 5: International Regulation of Virtual Currency and Blockchain</td>
<td>74</td>
</tr>
<tr>
<td>5.1 Virtual Currencies as Legal Tender or a Legal Method of Payment</td>
<td>74</td>
</tr>
<tr>
<td>5.2 Countries Where Virtual Currency is Banned</td>
<td>77</td>
</tr>
<tr>
<td>5.3 Chinese Government Actions Concerning Virtual Currency</td>
<td>78</td>
</tr>
<tr>
<td>5.4 Taxation of Virtual Currencies in Other Countries</td>
<td>80</td>
</tr>
<tr>
<td>5.5 International Anti-Money Laundering Laws That Affect Virtual</td>
<td>82</td>
</tr>
<tr>
<td>Currencies</td>
<td></td>
</tr>
<tr>
<td>5.6 Regulatory Sandboxes</td>
<td>86</td>
</tr>
<tr>
<td>Chapter 6: Anti-Money Laundering and Countering Terrorism Financing</td>
<td>95</td>
</tr>
<tr>
<td>6.1 The Basics of Money Laundering</td>
<td>95</td>
</tr>
<tr>
<td>6.2 Use of Virtual Currency in Money Laundering</td>
<td>96</td>
</tr>
<tr>
<td>6.3 Federal AML Framework</td>
<td>98</td>
</tr>
<tr>
<td>6.3.1 Bank Secrecy Act of 1970 and PATRIOT Act</td>
<td>98</td>
</tr>
<tr>
<td>6.3.1.1 Scope</td>
<td>99</td>
</tr>
<tr>
<td>6.3.1.2 AML Requirements</td>
<td>100</td>
</tr>
<tr>
<td>6.3.1.3 Penalties</td>
<td>102</td>
</tr>
<tr>
<td>6.3.1.4 FinCEN Guidance</td>
<td>103</td>
</tr>
<tr>
<td>6.3.1.5 FinCEN Enforcement Activity</td>
<td>104</td>
</tr>
<tr>
<td>6.3.2 Money Laundering Control Act of 1986</td>
<td>105</td>
</tr>
<tr>
<td>6.3.2.1 Section 1956</td>
<td>105</td>
</tr>
<tr>
<td>6.3.2.2 Section 1957</td>
<td>107</td>
</tr>
<tr>
<td>6.3.3 Prohibition of Unlicensed Money Transmitting Businesses</td>
<td>108</td>
</tr>
<tr>
<td>6.3.3.1 Virtual Currency Exchanges</td>
<td>109</td>
</tr>
<tr>
<td>Chapter 7: Cybercrimes</td>
<td>111</td>
</tr>
<tr>
<td>7.1 Hacking/Theft</td>
<td>111</td>
</tr>
<tr>
<td>7.1.1 Computer Fraud and Abuse Act of 1986</td>
<td>114</td>
</tr>
<tr>
<td>7.1.2 Cyberattacks on Blockchain Applications</td>
<td>117</td>
</tr>
<tr>
<td>7.1.2.1 The DAO</td>
<td>117</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>7.1.2.2</td>
<td>Coincheck</td>
</tr>
<tr>
<td>7.1.2.3</td>
<td>Mt. Gox</td>
</tr>
<tr>
<td>7.1.2.4</td>
<td>Bitfinex Bond Issuance</td>
</tr>
<tr>
<td>7.1.2.5</td>
<td>Youbit/Yapizon</td>
</tr>
<tr>
<td>7.1.2.6</td>
<td>Bithumb Data Breach</td>
</tr>
<tr>
<td>7.1.3</td>
<td>Cyber-risk Insurance for Losses</td>
</tr>
<tr>
<td>7.2</td>
<td>New York Cybersecurity Requirements for Financial Services Companies</td>
</tr>
<tr>
<td>8.1</td>
<td>Initial Coin Offerings</td>
</tr>
<tr>
<td>8.2</td>
<td>Investor Protection Issues</td>
</tr>
<tr>
<td>8.2.1</td>
<td>Offer and Sales of Digital Asset Securities</td>
</tr>
<tr>
<td>8.2.2</td>
<td>Investment Vehicles Investing in Digital Asset Securities</td>
</tr>
<tr>
<td>8.2.3</td>
<td>Trading of Digital Asset Securities</td>
</tr>
<tr>
<td>8.3</td>
<td>Securities Law Issues</td>
</tr>
<tr>
<td>8.3.1</td>
<td>The Howey Test</td>
</tr>
<tr>
<td>8.3.1.1</td>
<td>Investment of Money</td>
</tr>
<tr>
<td>8.3.1.2</td>
<td>Common Enterprise</td>
</tr>
<tr>
<td>8.3.1.3</td>
<td>Expectation of Profits</td>
</tr>
<tr>
<td>8.3.1.4</td>
<td>Solely from the Efforts of Others</td>
</tr>
<tr>
<td>8.3.2</td>
<td>SEC Report on The DAO</td>
</tr>
<tr>
<td>8.3.3</td>
<td>Crowdfunding Exemption for ICOs Below $1,000,000</td>
</tr>
<tr>
<td>8.3.4</td>
<td>Recent SEC Enforcement Actions and Class Actions for Unregistered ICOs</td>
</tr>
<tr>
<td>8.4</td>
<td>Simple Agreement for Future Tokens</td>
</tr>
<tr>
<td>8.4.1</td>
<td>Airdrops</td>
</tr>
<tr>
<td>8.5</td>
<td>International Developments</td>
</tr>
<tr>
<td>8.5.1</td>
<td>Canada</td>
</tr>
<tr>
<td>8.5.2</td>
<td>China</td>
</tr>
<tr>
<td>8.5.3</td>
<td>Hong Kong</td>
</tr>
<tr>
<td>8.5.4</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>8.5.5</td>
<td>Thailand</td>
</tr>
<tr>
<td>8.5.6</td>
<td>South Korea</td>
</tr>
<tr>
<td>8.5.7</td>
<td>Germany</td>
</tr>
<tr>
<td>8.5.8</td>
<td>Vietnam</td>
</tr>
<tr>
<td>8.5.9</td>
<td>European Union</td>
</tr>
<tr>
<td>8.5.10</td>
<td>Russia</td>
</tr>
<tr>
<td>8.5.11</td>
<td>Singapore</td>
</tr>
<tr>
<td>8.5.12</td>
<td>Switzerland</td>
</tr>
<tr>
<td>8.5.13</td>
<td>Australia</td>
</tr>
<tr>
<td>9.1</td>
<td>Electronic Funds Transfer Act (EFTA)</td>
</tr>
<tr>
<td>9.1.1</td>
<td>Prepaid Accounts Rule Exempts Virtual Currency</td>
</tr>
<tr>
<td>9.1.2</td>
<td>The Consumer Financial Protection Bureau’s Sandbox</td>
</tr>
<tr>
<td>9.2</td>
<td>Federal Reserve</td>
</tr>
</tbody>
</table>
Chapter 12: Data Management and Protections ................................................................. 190
9.2.1 Federal Guidance .................................................................................................. 158
  9.2.1.1 Federal Advisory Council and Board of Governors (5-9-2014) ..................... 158
  9.2.1.2 Strategies for Improving U.S. Payment Systems ............................................ 159
  9.2.1.3 Distributed Ledger Technology in Payments, Clearing and Settlement .......... 162
9.3 The Office of the Comptroller of the Currency (OCC) ............................................. 162

Chapter 10: Consumer Protection ............................................................................... 167
10.1 State Law .................................................................................................................. 167
10.2 Federal Law ............................................................................................................... 168
  10.2.1 The Federal Trade Commission Act of 1914 ................................................... 168
    10.2.1.1 Unfair Methods of Competition and Unfair or Deceptive Acts or Practices . 169
    10.2.1.2 Enforcement ............................................................................................. 170
    10.2.1.3 FTC’s Blockchain Working Group ............................................................... 171
  10.2.2 The Dodd-Frank Wall Street Reform and Consumer Protection Act .......... 172
  10.2.3 The Gramm-Leach-Bliley Act ............................................................................ 173
    10.2.3.1 Scope ........................................................................................................ 175
    10.2.3.2 Requirements .......................................................................................... 176
    10.2.3.3 Penalties .................................................................................................. 178
    10.2.3.4 Application to Blockchain Businesses ....................................................... 178

Chapter 11: Property ....................................................................................................... 180
11.1 Blockchain for Title Registry .................................................................................. 180
  11.1.1 Blockchain Technology Can Obviate the Need for Title Insurance in the U.S .. 181
    11.1.1.1 Accenture’s Editable Blockchain ............................................................... 182
  11.1.2 International Efforts to Implement Blockchain Land Registries ...................... 184
    11.1.2.1 Sweden ................................................................................................... 184
    11.1.2.2 Russia .................................................................................................... 185
    11.1.2.3 Georgia .................................................................................................. 186
    11.1.2.4 Ghana .................................................................................................... 187
  11.2 EDCCs for Real Estate Transactions ...................................................................... 187

Chapter 12: Data Management and Protections ................................................................. 190
12.1 Privacy Protections ................................................................................................. 190
    12.1.1 Relevant Federal Laws .................................................................................. 191
      12.1.1.1 The Wiretap & Electronic Communications Privacy Act ......................... 191
      12.1.1.2 The Privacy Act ..................................................................................... 194
      12.1.1.3 The Computer Fraud and Abuse Act ..................................................... 196
      12.1.1.4 The Identity Theft Penalty Enhancement Act ........................................ 197
      12.1.1.5 The Children’s Online Privacy Protection Act ....................................... 198
    12.1.2 Challenges to Privacy ...................................................................................... 200
      12.1.2.1 AML/KYC Requirements and PATRIOT Act ..................................... 200
12.2 Use of Blockchain Technology for Particular Types of Data ..................................... 201
    12.2.1 Blockchain for Storage of Health Records ................................................... 201
Chapter 1

1 The History of Virtual Currency

Introduced in 2008, Bitcoin was the first decentralized virtual currency, but it was hardly the first virtual currency. Long before Bitcoin’s introduction, individuals and companies were experimenting with and releasing various centralized virtual currencies.

1.1 Precursors to Decentralized Virtual Currencies

Over the past three decades, global access to and use of the Internet has increased significantly, spurring the growth of online commercial activity. Traditional methods of payment, however, have failed to meet the needs of this new global market. Tangible cash and checks, while suitable for payments at brick-and-mortar stores, pose special concerns for online retailers and consumers, including logistical issues (e.g., how to collect and deposit cash and checks) and lack of recourse for nondelivery or nonconformity. Credit cards, while used frequently by consumers and retailers, impose different burdens, such as authentication, trust, and recording requirements. Additionally, some of these payment methods, which generally involve intermediaries, can discourage participation by consumers who lack the credit histories required to open bank accounts, who fear invasion of their privacy or mistrust financial institutions, who cannot afford the costs associated with having an account, or who lack physical access to banks. Also, the cross-border transfer system is slow, error-prone, and costly, as transfers are facilitated by several financial institutions operating in different jurisdictions throughout the world, using different fiat currencies. To address these inadequacies, starting in the late twentieth century, several forward-thinkers began conceptualizing the development of an alternative payment system based on virtual currency.

Virtual currency can be convertible, non-convertible, or a hybrid thereof. Moreover, a convertible virtual currency can be centralized or decentralized, exchangeable for fiat currency, and used to purchase tangible or virtual goods and services. Conversely, a non-convertible virtual currency is centralized, not exchangeable for fiat currency, and only usable for purchasing virtual...
goods or services. A hybrid virtual currency has some, but not all, features of convertible or non-convertible virtual currencies. For example, a hybrid virtual currency may be purchased with fiat currency but not redeemed for fiat currency, as is typically the case in multiplayer online role-playing games.

A centralized virtual currency is issued by a single authority responsible for controlling its circulation and maintaining ownership and transaction records. By contrast, a decentralized virtual currency has no central authority; it is issued pursuant to the system protocol, and every user in a decentralized system maintains the ownership and transaction records. A virtual currency, whether centralized or decentralized, that verifies the transfer of value, secures transactions, and controls the creation of additional units of the currency through cryptography is called a “cryptocurrency.”

What follows is a brief historical overview of how centralized virtual currencies evolved into decentralized virtual currencies such as bitcoin and Ether.

1.1.1 E-Cash

In 1990, inventor and cryptographer David Chaum created E-Cash through his company DigiCash Inc. E-Cash implemented blind signature technology, a method for making untraceable payments that Chaum had invented back in 1983 to help ensure the privacy of users who conduct online transactions. In May 1994, Chaum sent the world’s first electronic cash payment over a computer network using E-Cash.

Chaum strongly believed in cryptography and privacy-enhancing technologies as a route to social and political change. He was concerned about companies’ ever-increasing ability to amass user data and about the security of such data. Chaum envisioned E-Cash as an electronic payment

---

6 Id. at 4.
7 Id.
10 As Chaum summarized: “A new kind of cryptography, blind signatures, has been introduced. It allows realization of untraceable payments systems which offer improved auditability and control compared to currency systems, while at the same time offering increased personal privacy.” David Chaum, Blind Signatures for Untraceable Payments, 203 (1983), http://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.
method that would have the same attributes as paper cash with respect to privacy and untraceability.

E-Cash is best described as electronic cash backed by fiat currency. The system was tied to a bank, as a trusted third party, and required user software in order to withdraw or transfer funds using encrypted keys.\textsuperscript{13} This advancement of public and private key cryptography made electronic payments untraceable by the issuing bank, while still permitting the bank to detect double-spending and ensure the validity of electronic payments.\textsuperscript{14}

DigiCash pioneered e-commerce through its introduction of E-Cash but ultimately failed due to its inability to scale and expand its user base.\textsuperscript{15} DigiCash filed bankruptcy in 1998 and was forced to sell off all assets, including its patents.\textsuperscript{16}

\subsection*{1.1.2 E-Gold}

In 1996, Douglas Jackson founded E-Gold, a forerunner to today’s virtual currencies that reportedly had one million client accounts by November 2003.\textsuperscript{17} E-Gold was an Internet-based system in which users made payments denominated in gold or other precious metals, which the company claimed were secured by actual gold bullions that it held.\textsuperscript{18}

E-Gold ultimately experienced significant legal troubles due to its failure to register as a money transmitter under U.S. federal regulations. As a result, on April 24, 2007, a federal grand jury issued a four-count indictment charging E-Gold and its owners with violations of state and federal laws against money laundering and for operating as a money transmitter without an appropriate license.\textsuperscript{19}

E-Gold’s lawyers sought to dismiss the indictment, arguing that the defendants were not operating as a money transmitting business under 18 U.S.C. § 1960 because the indictment failed

\begin{flushleft}
\textsuperscript{13} Id.  \\
\textsuperscript{14} Id.  \\
\textsuperscript{15} According to Chaum, “It was hard to get enough merchants to accept it, so that you could get enough consumers to use it, or vice versa.” Jens-Ingo Brodesser, \textit{Interview with David Chaum, Founder, DigiCash Inc.}, First Monday (July 5, 1999), \url{http://firstmonday.org/ojs/index.php/fm/article/view/683/593}; see also Julie Pitta, \textit{Requiem for a Bright Idea}, Forbes (Nov. 1, 1999), \url{http://www.forbes.com/forbes/1999/1101/6411390a.html}.  \\
\end{flushleft}
to allege that they had engaged in cash transactions. The court rejected this argument, finding that the definition of “money-transmitting business” was sufficiently broad that defendants were still subject to currency reporting requirements even if E-Gold never handled cash. Jackson ultimately pled guilty, and E-Gold discontinued operations.

1.1.3 B-Money

In 1998, “an anonymous, distributed electronic cash system” called “B-money” was proposed by Wei Dai. B-money was considered the first system to publicly broadcast all transactions and propose the use of a proof-of-work function as a means of creating B-money.

Essentially, Dai proposed the idea for the world’s first cryptocurrency. As he explained: “Anyone can create money by broadcasting the solution to a previously unsolved computational problem. The only conditions are that it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual.”

B-money received little attention from the academic community, and Dai never built a functioning system. However, the ideas he proposed set the stage for future innovation.

1.1.4 WebMoney

Established in 1998, WebMoney is a settlement system for conducting online business activities. Users of WebMoney can keep track of their funds, attract funding, resolve disputes, and make secured transactions using WM, the system’s centralized virtual currency. WebMoney works like a prepaid debit card where the user purchases WM units in fiat currency and can then transact electronically with other WM unit holders.

Initially, WebMoney allowed users to register and transact on its platform while maintaining complete anonymity. In 2010, however, WebMoney increased security on its platform by requiring users to verify their identity.

---

21 As the court explained in E-Gold, “Section 1960 defines ‘money transmitting’ broadly to include transferring ‘funds,’ not just currency, by ‘any and all means;’ it is not limited to cash transactions.” Id. at 88. Accordingly, “[t]he term ‘money transmitting business’ as used in Section 5330 includes all financial institutions that fall outside of the conventional financial institutions system (and that are not a ‘depository institution’), not just those that engage in cash transactions.” Id. at 93.
25 Dai, supra note 23.
26 Bonneau, supra note 24.
by requiring users to provide identifying information during the registration process. As of 2018, WebMoney is still in existence and claims over 36 million users worldwide.

1.1.5 Linden Dollars

In 2002, Linden Lab released Second Life, a massive multiplayer online game through which users access a marketplace where Linden dollars, the company’s centralized virtual currency, can be used to purchase in-game items. Users can freely exchange and convert Linden dollars into fiat currency outside of this virtual economy. The intrinsic value of Linden dollars is rooted in their utility to gameplay in the Second Life virtual world.

In 2017, Linden Lab reported that Second Life had “between 800,000 and 900,000” active monthly users and an in-game gross domestic product (“GDP”) (i.e., the value of all goods and services produced in the game) of around $500 million.

1.1.6 Bit Gold and Reusable Proof-of-Work

In 2005, Nick Szabo proposed the creation of Bit Gold, a virtual currency where the value did not depend on trust in a third party, such as a government, bank, or clearinghouse. Instead, the virtual currency’s value stemmed from its unforgeable scarcity due to the costliness of its creation, a characteristic similar to precious metals and collectibles.

Szabo intended to automate the characteristics of precious metals and collectibles through software. His proposal was to create a string of bits where a previously created bit would serve as

---

28 Id.

29 Id.


31 Id.


34 Szabo, Bit Gold, supra note 33.

35 In 2002, Szabo published his theory of collectibles, in which he attributed cooperation between people to the development of the precursors of money (i.e., beads, necklaces) sharing similar characteristics: (1) security from accidental loss and theft; (2) costliness to forge; and (3) valuation accurately approximated through simple observation or measurement. Nick Szabo, Shelling Out: The Origins of Money, Satoshi Nakamoto Institute (2002), http://nakamotoinstitute.org/shelling-out/.
the basis for the next bit, using proof-of-work functions similar to Dai’s B-money.\textsuperscript{36} Bit Gold was designed to be limited in supply. As time passed, these computations would become increasingly difficult, requiring additional computing power, so that new units of Bit Gold would be costlier to create.

Szabo’s proposal of Bit Gold was principally a call for a deflationary decentralized cryptocurrency that did not require a trusted third party as an intermediary; however, Bit Gold never gained sufficient support to attain fruition.\textsuperscript{37}

In 2004, Harold “Hal” Thomas Finney II created a prototype based on Szabo’s theory of collectibles, called Reusable Proof-of-Work (RPOW),\textsuperscript{38} which was designed to serve a large network.\textsuperscript{39} RPOW became the first “digital collectible to ever function as a piece of software” but never achieved widespread acceptance.\textsuperscript{40}

\subsection*{1.1.7 Liberty Reserve}

Established in 2006, and incorporated in Costa Rica, Liberty Reserve was a centralized digital currency electronic transfer service backed by dollars or euros that allowed users to transact anonymously.\textsuperscript{41} Liberty Reserve ceased operations in May 2013, due to government seizure\textsuperscript{42} of its website following the arrest of its owner, Arthur Budovsky, as part of a joint money laundering investigation by law enforcement in the United States and Costa Rica.\textsuperscript{43} Budovsky ultimately pled guilty to one count of conspiring to commit money laundering and received a prison sentence of 20 years.\textsuperscript{44}

\begin{itemize}
  \item Szabo, \textit{Bit Gold}, supra note 33.
  \item See Hal Finney, \textit{RPOW - Reusable Proofs of Work} (Aug. 16, 2004), \url{http://cryptome.org/rpow.htm}.
  \item RPOW – Reusable Proofs of Work, Satoshi Nakamoto Institute (2004), \url{http://nakamotoinstitute.org/finney/rpow/}.
  \item Id.
  \item Liberty Reserve, \textit{Terms of Service}, § 1.7 (Aug. 8, 2012).
  \item Behind MLM, Liberty Reserve Shut Down for “Money Laundering,” (May 25, 2013), \url{http://behindmlm.com/mlm/liberty-reserve-shutdown-for-money-laundering/}.
  \item See Press Release, U.S. Dept. of Justice, Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court to 20 Years for Laundering Hundreds of Millions of Dollars
\end{itemize}
Prior to the government seizure, Liberty Reserve had more than one million users worldwide, who had conducted approximately 55 million transactions through its system totaling more than $6 billion in funds.45

1.1.8 M-Pesa

In March 2007, Safaricom,46 Kenya’s largest cell phone provider, released M-Pesa, an app that allows customers to use their mobile phones to transfer and receive funds, pay bills, pay for goods, save and borrow money, and complete bank transactions.47

Use of M-Pesa in Kenya has grown substantially. In 2007, mobile payment transactions represented less than 1% of the country’s GDP. By 2016, that figure had skyrocketed to approximately 48% of GDP.48 M-PESA has now expanded to nine other countries: Albania, Democratic Republic of Congo, Egypt, Ghana, India, Lesotho, Mozambique, Romania, and Tanzania.49

To use the platform, a customer downloads the M-PESA app to their mobile phone, opens an account in person through an authorized M-PESA agent, and deposits fiat currency with the agent in exchange for electronic cash.50 The customer may then transfer funds to a recipient by inputting a PIN and the recipient’s phone number into the app.51 The M-PESA platform sends a

---


46 Safaricom is partly owned by Vodafone.


51 Safaricom, supra note 50.
transfer confirmation to both customer and recipient. A customer can withdraw funds either by visiting an M-PESA agent, showing identification, and entering a PIN, or from an ATM by entering a PIN and a special one-time authorization code generated for ATM withdrawals.\footnote{Id.}

Non-registered M-PESA customers who receive an M-PESA transfer may exchange the electronic cash for fiat currency by presenting the transfer confirmation to an M-PESA agent. The transfer confirmation will display a one-time code for use by the agent, which serves as an extra security feature.\footnote{Id.}

### 1.1.9 SUCRE

In 2009, certain member countries of the Alianza Bolivariana para los Pueblos de Nuestra América (“ALBA”) signed a treaty establishing the Sistema Unitario de Compensación Regional de Pagos (“SUCRE”), a centralized virtual currency used in commercial transactions between these members.\footnote{ALBA countries include Antigua and Barbuda, Bolivia, Cuba, Dominica, Ecuador, Grenada, Nicaragua, Saint Kitts and Nevis, Saint Lucia, St. Vincent and the Grenadines, and Venezuela.}

Currently, SUCRE is used by Nicaragua, Venezuela, Ecuador, Cuba, and Bolivia.

SUCRE is used between member countries exclusively for large-scale commercial imports and exports, such as Bolivia’s 2010 sale of 5,000 tons of soy oil to Venezuela for 4.46 million SUCREs.\footnote{Patricia Rey Mallen, \textit{A Latin American Euro? The Region’s First Steps Towards A Unique Currency – What Is The Sucre?}, IBT Times (Jun. 7, 2013), \url{http://www.ibtimes.com/latin-american-euro-regions-first-steps-towards-unique-currency-what-sucre-1296787}.} The virtual currency is not available to individual citizens of the ALBA countries for personal transactions. It is meant to function alongside the national currencies of the member countries and not to replace them.

### 1.2 Decentralized Virtual Currencies

#### 1.2.1 Bitcoin

Bitcoin is the world’s first successful decentralized virtual currency. It is an innovative payment network and new kind of payment system that operates according to pre-defined rules and protocols rather than the politics of traditional government-backed currencies.

Bitcoin has long been shrouded in mystery. The person (or group) responsible for its creation remains anonymous, using only the pseudonym Satoshi Nakamoto. In November 2008, Nakamoto released a research paper, via the Cryptographic and Cryptography Policy Mailing List,\footnote{The Cryptography and Cryptography Policy Mailing List, \url{http://www.metzdowd.com/mailman/listinfo/cryptography} (last visited Oct. 18, 2018).} titled “Bitcoin: A Peer-to-Peer Electronic Cash System.”\footnote{Satoshi Nakamoto, \textit{Bitcoin: A Peer-to-Peer Electronic Cash System}, \url{http://bitcoin.org/bitcoin.pdf} (last visited Oct. 18, 2018).} In it, Nakamoto noted that commerce transacted over the Internet relies “almost exclusively on financial institutions serving

\footnote{\textit{Id.}}

\footnote{\textit{Id.}}

\footnote{ALBA countries include Antigua and Barbuda, Bolivia, Cuba, Dominica, Ecuador, Grenada, Nicaragua, Saint Kitts and Nevis, Saint Lucia, St. Vincent and the Grenadines, and Venezuela.}


\footnote{The Cryptography and Cryptography Policy Mailing List, \url{http://www.metzdowd.com/mailman/listinfo/cryptography} (last visited Oct. 18, 2018).}

as trusted third parties to process electronic payments.” Nakamoto’s proposed system sought to eliminate the inherent weakness of the trust-based model, which accepts a certain percentage of fraud as unavoidable.

Bitcoin was officially released to the public for download in 2009. Until its release, a decentralized program for making payments over a communications channel without a trusted third party had never existed.

Bitcoin operates on a peer-to-peer (P2P) network using a consensus-forming algorithm that processes and clears transactions on an immutable, shared public ledger known as the “block chain” or “blockchain.” Bitcoin has no central issuer; rather, the P2P network secures existing bitcoins, controls the generation of new coins, and confirms transactions through a competitive and decentralized process known as “mining,” which requires expending resources to solve a difficult proof-of-work problem. By design, the total number of bitcoins that can ever be mined is capped at 21 million, a limit that will likely be reached by the year 2140.

As of December 2018, approximately 16.522 million bitcoins were in circulation. The market price of one bitcoin was approximately $6,632.00 with market capitalization of approximately $114 billion, the highest of any cryptocurrency. Bitcoin has emerged as the most successful and widely used cryptocurrency in history, even though it is backed by nothing but the computing power and resources that comprise the system.

1.2.2 Ethereum

Ethereum is a public, blockchain-based, distributed computing platform that was proposed by Vitalik Buterin in 2013. Like Bitcoin, Ethereum utilizes public key cryptography and a blockchain powered by miners through a peer-to-peer decentralized network of computers.

---

58 Id.
59 Id.
62 BitcoinWiki, supra note 61.
64 A bitcoin (BTC) can be denominated to one hundred millionths of a single bitcoin, (0.00000001) or (10^-8). This denomination is called a “Satoshi,” the smallest unit of a bitcoin used in a transaction.
Ethereum, however, goes much further because it is not solely a decentralized payment system like Bitcoin but rather a programmable blockchain allowing users to create their own applications on the platform.

In 2014, a crowdsale raised approximately $18.5 million worth of bitcoin, and the Ethereum Foundation, a Swiss non-profit, was formed to manage those funds. The Ethereum platform was eventually released on July 30, 2015.

As of December 2018, approximately 104 million Ether are in circulation\(^67\) and market capitalization is in excess of $23 billion,\(^68\) the second highest of any cryptocurrency.\(^69\)

1.2.3 Dash

Dash or Digital Coin, formerly known as Darkcoin and Xcoin, is a cryptocurrency based on Bitcoin software.\(^70\) Dash claims to offer greater privacy than bitcoin via a service called PrivateSend that combines inputs from multiple users into a single transaction with multiple outputs, thereby obscuring the origins of the Digital Coins used therein.\(^71\) Dash also provides a service called InstantSend, which processes transactions almost instantaneously.\(^72\)

Based on its governance structure, Dash considers itself to be the first decentralized autonomous organization.\(^73\) A small portion of each block reward is dedicated to funding developments and projects, which are voted on by owners of the organization’s masternodes.\(^74\) As of October 2018, the market capitalization of the Dash token was nearly $1.52 billion.\(^75\)

\(^68\) Id.
1.2.4 Ripple

Ripple is a decentralized payment system that utilizes its cryptocurrency, XRP, to effectuate transfer of value across borders. In Ripple’s view, the global payment infrastructure is slow, error-prone, and costly because transactions occur across different systems, involving numerous intermediaries and various currencies.76 The Ripple protocol ameliorates these issues through the use of XRP, which functions as a “universal bridge asset.”77 By using XRP to make cross-border payments, banks free themselves from having to hold various fiat currencies in local accounts, thus reducing liquidity costs. Ripple also reduces delays and errors by minimizing the number of intermediaries involved in making cross-border payments.78

As of December 2018, the market price for an XRP token was approximately $0.3567, and the market capitalization of the XRP token was in excess of $35 billion.79

76 Ripple, supra note 4.
77 Id.
78 Id.
Chapter 2

2  Blockchain Technology

2.1  Public Key Cryptography

Decentralized virtual currencies use public key cryptography (also referred to as “asymmetric key cryptography”), which serves both cryptographic and digital signature functions. Unlike symmetric key cryptography, which uses one key to both encrypt and decrypt, public key cryptography is based on a pair of mathematically linked keys (essentially long strings of letters and numbers). One key is private and known only to the owner, while the other is public and may be shared with others. Using software, it is possible to derive the public key from its private counterpart. But it is nearly impossible to do the reverse and use the public key to determine the private. These public and private keys can be thought of as an account number and password, respectively.

2.1.1  Encryption

The value of public key cryptography is that it allows people with no pre-existing security arrangement to communicate and securely exchange information via encryption.

To encrypt the data in a message, a sender uses the recipient’s public key as a cipher to translate the plain data into a string of letters and numbers. This encrypted data is then sent to the recipient, who uses his or her corresponding private key to decrypt the message, which is then readable by the recipient. Only the corresponding private key will decrypt the message. Security depends on the recipient keeping the private key private; the public key may be disclosed without compromising security.

2.1.2  Digital Signatures

Public key cryptography can also be used to create digital signatures that permit the recipient to verify the sender of a message. Bitcoin and Ethereum use Elliptic Curve Digital Signature Algorithm (“ECDSA”) to validate transactions. To digitally sign a message, the

---


82 Id.


84 See Brito, supra note 80.

85 See Asymmetric Cryptography, supra note 81.

sender’s software program first translates the message into a string of letters and numbers of a
given length, a process known as “hashing.”87 The resulting string of letters and numbers is called
a “digest” and is practically impossible to reverse (in contrast to an encrypted message, which can
be decrypted).88 The sender’s software then combines the sender’s private key with the digest and
runs the combination through the ECDSA to create another hash.89 Using the sender’s public key
and message data, the recipient’s software program can then mathematically verify that the digital
signature is in fact the sender’s.90 Since this digital signature is message-specific insofar as it partly
includes the message, it may not be used for another transaction, and any attempt to alter the digital
signature will invalidate it. This cryptographic element provides user anonymity and security
against forgery.91

As explained by cryptographer David Chaum: “The immensely useful property of digital
signatures is their resistance to ‘forgery.’ . . . [W]ith actual digital-signature cryptographic
techniques currently in use, forgery is thought to require so much computation as to be infeasible
even for the fastest computers working for millions of years. If an organization cannot forge a
digital signature of yours, then it cannot successfully claim that you sent it a message that you in
fact did not send.”92 By that same token, this feature also eliminates the problem of message
senders later disavowing their messages.93

2.2. Blockchain

2.2.1 Blockchain as a Ledger of Transactions

Blockchain technology acts as an immutable virtual ledger that records all verified digital
transactions and messages sent within a particular peer-to-peer network of computers connected
through the same software.94 Each computer on the network is referred to as a “node.”95 Blockchains have the capacity to record and organize a multitude of digital transactions, such as

87 Victor S. Adamchick, Concept of Hashing, Carnegie Mellon University (2009),
88 Public Key Encryption and Digital Signature: How do they Work?, CGI White Paper (2004),
https://www.cgi.com/files/white-papers/cgi_whpr_35_pki_e.pdf.
89 Id.
90 Id.
91 See Brito, supra note 80.
92 David Chaum, Security Without Identification: Transaction Systems to Make Big Brother
Obsolete, 28 Commc’n’s of the ACM 1030, 1033-34 (1985),
93 Id.
94 Sloane Brakeville and Bhargav Perepa, Blockchain Basics: Introduction to Distributed
Ledgers, IBM (Mar. 18, 2018), https://www.ibm.com/developerworks/cloud/library/cl-
blockchain-basics-intro-bluemix-trs/index.html.
95 Id.
transfers of virtual currency, health records, or records on the origins of food products. The essence of a blockchain’s operation is that, whenever two nodes on the network transact, the sender broadcasts the transaction to all network members, who acknowledge and record the transaction.

When recording a digital transaction on a blockchain, a mathematical function turns the transaction data into a hash. Several hashed transactions then wait to be imprinted on a block until the block reaches its limit of 4 MB. Once a block is full, the transactions in that block are verified through the mining process.

The mining verification process varies depending on the blockchain network. For example, the Bitcoin and Ethereum blockchains are “permissionless,” meaning they are public in that every node has a copy of the blockchain. Other blockchain networks, however, can operate on a “permissioned” basis – i.e., while anyone may have a copy of the blockchain, only certain nodes are allowed to validate block transactions. Blockchain networks can also be private, limiting those with access to the blockchain.

Verification through consensus, timestamping, and recordation on the blockchain solve the “double-spend” problem, where a person can, unlike with cash, potentially spend the same digital representation of value more than once. For example, if Alice pays a merchant, Bob, $5 in cash for a cup of coffee, then she cannot spend that same $5 unless she steals the $5 back. However, a digital representation of value may be copied as simply as copying and pasting a computer file, permitting it to be spent more than once. For example, if Alice sends an email to Bob and attaches $5 in digital form as a computer file, she retains a copy of that $5 in digital form and can later send

99 A sender may rebroadcast a transaction if it fails to propagate on the network. This can happen if the sender’s transaction fee provides insufficient incentive for miners to include the transaction on a block, see Section 2.5, or if the sender suffers technical problems. Rebroadcasting can be done manually by the sender or automatically by the sender’s wallet. Mark, How to Rebroadcast a Bitcoin Transaction Using Blockchain.info’s PushTx Feature, The Merkle (Dec. 2, 2015), https://themerkle.com/how-to-rebroadcast-an-electrum-transaction-using-blockchains-pushtx/.
100 See Adamchick, supra note 87.
101 See Section 2.5.1.
102 See Section 2.5.2.
104 Id.
105 Id.
it to a second person, Chris, without Bob or Chris knowing about each transaction, and without either of them being able to verify the authenticity of the digital $5 sent.

If this same transaction is conducted through the Ethereum network, Alice cannot spend the same Ether twice. For example, if Alice transmits $5 worth of Ether to Bob, then that transaction is timestamped and recorded on the blockchain to reflect that Bob now owns the $5 worth of Ether. If Alice later tries to send the exact same Ether to Chris, the transaction will fail, since the network will show that Bob, not Alice, owns that Ether. Similarly, if Alice tries to transmit the $5 worth of Ether to Bob and Chris simultaneously, whichever transaction gets recorded on the blockchain first will successfully effectuate the transfer of Ether. The second will fail.

2.2.2 The Mining Process and Verification of Transactions

Transactions, such as transfers of the cryptocurrencies bitcoin or Ether, are verified and added to the blockchain through a process called “mining,” whereby computer hardware runs mining software to solve complex mathematical problems.106 Transactions are first sent to a miner’s mempool, a memory storage where pending transactions wait.107 Miners then select which transactions they want to include in the block they mine.108 During this process, each computer in the network reviews its copy of the blockchain to verify a transaction’s authenticity.109

Thousands of transactions are verified concurrently and grouped together into a block.110 For the block to be validated, the first miner to solve the algorithm publishes the answer to all other miners on the network.111 If and when a consensus is reached that this solution is correct, the block is timestamped and recorded on the blockchain.112 Validation of each block on the Bitcoin blockchain takes about 10 minutes, whereas the Ethereum block time is 24-25 seconds.113

The miner who first solves an algorithm collects a “block reward” in the form of newly minted virtual currency, as well as any fees associated with the transactions included on the

107 Id.
108 See Section 2.5.1.
110 In the Bitcoin network, each block typically contains between one and two thousand transactions. See Blockchain.info, *Average Number of Transactions per Block*, https://blockchain.info/charts/n-transactions-per-block (last visited Sept. 25, 2018).
112 Id.
block. With Bitcoin, the block reward, which was originally 50 bitcoin, is halved every 210,000 blocks, or approximately every four years at the current rate, in order to control the currency supply, which is limited to 21 million bitcoins. Ethereum block rewards are not halved, and there is no limit on the total supply of Ether.

Given the increasing competition to solve the equations that confirm blockchain transactions, miners frequently group their computing power into mining pools, which increase their chances of successfully solving these algorithms first and thereby reaping the block rewards.

2.2.2.1 Peer-to-Peer Network

Mining is performed through a peer-to-peer (P2P) network, a type of decentralized and distributed network architecture in which individual nodes, called “peers,” act as both suppliers and consumers of resources. This is in contrast to the centralized client-server model used by all virtual currencies that preceded bitcoin, where nodes request access to resources provided by central servers. In a P2P network, there are no fixed clients or servers; instead, each computer acts as both client and server. This decentralized model was developed so that no one person or entity could control the protocol, which operates based on a distributed network consensus of peers. A P2P network eliminates the central point of control found in the client-server model, a feature that leaves centralized systems vulnerable to disruptive or disabling attacks.

There are different types of P2P networks. In the Napster music sharing network, for example, peers are responsible for storing information, but information about the network (e.g., the address of each peer) is stored on a central server. This requires a peer to send an inquiry to

---


119 *Id.*


121 *Id.*

122 *Id.*
the central server in order to communicate with another peer. Another type of P2P architecture (e.g., that used in the Bitcoin protocol) has no central server, relying instead on each peer to act as both client and server. A third type, like the decentralized file-sharing network Gnutella, has no central server but gives certain peers greater dominance in the network.

### 2.2.2.2 Proof-of-Work

The Bitcoin mining process uses the Hashcash proof-of-work algorithm, which is a consensus algorithm used not only to authenticate, secure, and track bitcoins already in existence but also to issue newly minted bitcoins via block rewards. In the proof-of-work process, miners authenticate their verifications of blocks by proving to the satisfaction of other miners in the network that they have spent computing power, and therefore energy, in performing this process. A miner does so by solving an algorithm, which basically entails guessing what inputs would result in a specific hash value. This process is difficult and resource-intensive, requiring computers to perform approximately $10^{21}$ computations. Once the algorithm is solved, the miner broadcasts the answer to the network for verification.

Verification requires simply that other miners run the solution (i.e., the inputs) through the same algorithm, using the same software as all other miners, to generate a hash that is then checked against the expected hash value. Once this solution is accepted by the others, the new block is linked chronologically to the previously solved blocks, creating a blockchain.

---


124 *Id.* at 383.

125 *Id.* at 384.

126 Hashcash proof-of-work was invented in 1997 by Adam Back to prevent spamming, denial of service attacks, and general network abuse. The idea is premised upon the fact that cryptographic hashes are very difficult to invert because a full hash inversion has a computationally infeasible brute-force running time. Bitcoin uses this technology to validate transactions and mint new coins. *See* Hashcash.org, *Hashcash*, [http://www.hashcash.org/](http://www.hashcash.org/) (last visited Oct. 10, 2018).


129 The inputs consist of the hash of the previous block, the current block of transactions to be processed, and a random number referred to as a “nonce” or “number used once.” In solving the algorithm, the miner tries to determine the nonce value that would generate a hash that solves the algorithm.


131 *See* Section 2.2.2.
Each completed Bitcoin block varies from 2 to 4 MB, containing a timestamp, the “nonce” (i.e., answer) to the algorithm, the hash value of the previous block, and a list of the transactions. The Ethereum blockchain is somewhat similar to that of the Bitcoin blockchain. The primary differences are that Ethereum blocks are limited by a block gas limit, rather than size, and contain a copy of both the transaction list and the most recent state, in addition to the block number and level of difficulty of the proof-of-work.

The longest chain serves not only as proof of the sequence of events, but also as proof that it comes from the largest pool of computing power. The processing power of the computers used to confirm virtual currency transactions is measured by their “hash rate” or number of calculations performed per second. The higher a computer’s hash rate, the greater its chance of solving the confirmation algorithm and ultimately receiving the block reward.

### 2.2.2.3 Proof-of-Stake

Proof-of-Work consumes many resources (e.g., electricity), because success is generally based on the volume of computational resources that go into processing and verifying a block. According to researchers, the rate of energy consumed in December 2018 by the Bitcoin network was equivalent to about 42.65 TWh per year, only slightly more than the amount of energy consumed by the entire state of Kansas in 2017. The Ethereum network consumed

---


133 See Acheson, *supra* note 130.


135 As used here, “state” refers to the ownership status of all existing Ether.


137 *Id*.


approximately 9.35 TWh per year, slightly more than the total energy consumed by the state of Hawaii in 2017.

Ethereum currently uses the Proof-of-Work (PoW) consensus algorithm, but Ethereum Foundation developers plan to eventually switch to a Proof-of-Stake (PoS) algorithm called Casper. The transition from PoW to PoS will occur through what Ethereum core developers have labeled the “Difficulty Bomb” – an increase in the difficulty of puzzles in the mining algorithm used to reward miners. As the puzzle becomes increasingly difficult, a substantial lag arises between the production of new blocks on the Ethereum blockchain. This lag makes the blockchain less attractive to miners and thus facilitates a transition to PoS. In addition, on August 31, 2018, the Ethereum core developers voted to reduce the block reward from three Ether to two Ether in an attempt to further discourage the PoW concept. The Difficulty Bomb is expected to be put into effect 12 months from the Ethereum Constantinople system upgrade. While the upgrade was expected to occur in 2018, it may be delayed because Ethereum developers discovered a bug in Constantinople’s code during a testnet upgrade.

PoS is an alternative consensus algorithm that is not based on computer processing power or the solving of algorithms. In PoS, there is no mining and thus no large-scale consumption of energy.


147 Id.

148 Id.


150 Id.


electricity. Instead, transactions are verified by “validators,” users who own the network tokens. Validators place a share of their tokens as collateral (sometimes called a “stake” or “bond”), which is “locked,” i.e., the validators cannot use it until the block is validated.

In validating blocks, validators bet their deposits on the expected results of the consensus process. Once a block is validated, the collateral is released to the validators, and their reward is based on the number of tokens staked and the correctness of their bet. Depending on the type of PoS, the algorithm may randomly assign a validator the right to create a block, or it may assign this right to several validators. Malicious validators who violate rules, by voting multiple times to influence a voting result, for example, forfeit their collateral.

Casper was proposed in 2015. Ethereum Foundation researcher Justin Drake confirmed in July 2018 that Casper, which is being developed as an executable distributed code contract, will likely launch in 2019.

### 2.2.2.4 Cloud Mining

Miners can, as an alternative to using their own hardware, mine bitcoin and other virtual currencies using shared processing power from data centers. This “cloud” mining allows miners to operate without needing to maintain hardware or pay the associated costs. Along the same lines, cloud mining reduces miners’ control over their operations and exposes them to potential fraud and abuse because miners pay data center operators based on promises of a certain amount of returns without verifying that the operators are legitimate businesses.

### 2.2.3 GHOST and Uncles

During the mining process, two blocks may be mined at the same time by different miners. This occurs more often with networks that have fast block times, such as Ethereum, because blocks are being mined so quickly. If blocks are mined simultaneously, the network will temporarily have

---

153 Id.
156 Id.
157 Id.
two chains. Eventually, though, subsequent blocks will be added to one of the chains, and the chain with the largest total proof-of-work (i.e., the “longest” chain) will be adopted. The block that does not get included onto the longest chain is considered stale, and the miner that mined this stale block collects no block reward or transaction fees. Transactions on the stale block will not be completed; thus, the resources used to mine stale blocks are wasted.

Ethereum terms these stale blocks “uncles” and assigns them some value in recognition that they are valid blocks that just happened not to be included on the longest chain. Ethereum adopted the Greedy Heaviest Observed SubTree (GHOST) protocol, which includes uncles “in the calculation of which chain is the ‘longest;' that is to say . . . which block has the largest total proof of work backing it.” Ethereum also allows a fraction of the block reward to go to the miner of the uncle, though the miner is still not entitled to any transaction fees.

2.3 Tokens

In the Bitcoin virtual currency system, bitcoin serves as a store of value. A unit of bitcoin may be divided in numerous ways, with the smallest fraction – one hundred millionth of one bitcoin (0.00000001 BTC) – called a Satoshi. Bitcoins are created through the mining process described above. As of December 2018, approximately 16.5 million bitcoins had been mined and were in circulation. By design, no more than 21 million bitcoins can ever be mined in total.
with all bitcoins expected to be fully issued by the year 2140.\textsuperscript{171} As of December 2018, the market capitalization of bitcoin was in excess of $67 billion, the highest of any cryptocurrency.\textsuperscript{172} Even though it is backed by nothing but the computing power and resources that make the system run, bitcoin has emerged among cryptocurrencies as the most successful and widely used.

The token used on the Ethereum network is called an Ether. Although Ether has value due to its scarcity and functional use, its main purpose is to pay for the computation and transaction fees associated with conducting transactions on applications built on the Ethereum network.\textsuperscript{173} One Ether can be denominated into a “Finney” (10\textsuperscript{-3}), “Szabo” (10\textsuperscript{-6}), and a “Wei” (10\textsuperscript{-18}).\textsuperscript{174} Ether is expected to be used for ordinary transactions, Finney for micro-transactions, and Szabo and Wei for technical discussions around fees and protocol implementation. Unlike bitcoin’s 21 million cap, there is no limit on how much Ether can ever exist. However, the developers have limited new supply to 18 million per year.\textsuperscript{175}

\subsection*{2.4 Wallets}

Cryptocurrency wallets allow users to store private keys and addresses associated with their virtual currency. Wallets may be online (with a virtual currency exchange, such as Coinbase, or a wallet provider, such as Blockchain), on a user’s desktop,\textsuperscript{176} or on a mobile phone app (e.g., Xapo).

Users may also keep private keys and addresses in cold storage, which are physical wallets not connected to the Internet. Cold storage may be in the form of hardware devices or paper wallets.\textsuperscript{177} Because the wallets are offline, cold storage protects against unauthorized access and cyberattacks. However, users who keep private keys and addresses in cold storage must remember the location of their physical wallets, because the private keys inside are the only way for them to access their virtual currency.


\textsuperscript{175} Id.

\textsuperscript{176} For example, the Bitcoin Core software, which a user downloads onto their computer, contains a wallet feature. See Bitcoin.org, supra note 115.

\textsuperscript{177} Hardware wallets, like those by Trezor (https://shop.trezor.io) and Ledger Wallet (https://wwwledgerwallet.com), function similarly to USB devices. Paper wallets are public and require private keys that are printed as two QR codes on separate pieces of paper. When users transact with the virtual currencies stored on paper wallets, they scan the QR codes using their mobile phones. Coindesk, How to Make a Paper Bitcoin Wallet, https://www.coindesk.com/information/paper-wallet-tutorial/ (last visited Sept. 25, 2018).
MyEtherWallet (MEW) is an open source service that interfaces with the Ethereum blockchain. Through MEW, users can generate wallets that are saved to their computer and store private keys to their Ether as well as ERC20 tokens issued through initial coin offerings. Users can make transactions while online or offline.

2.5 Transaction Fees

2.5.1 The Bitcoin Network

As stated previously, the block size on the Bitcoin blockchain ranges from 2 to 4 MB. Thus, while thousands of transactions are placed on a given block, thousands more are always pending in miners’ mempools. Miners select which transactions to include on a block and prioritize transactions based on several factors, including the amount of associated transaction fees.

Transaction fees are voluntary, meaning the sender can set any fee or none at all. But the process is competitive, and miners are more likely to pick transactions with fees associated than those without. In calculating the amount of fee to pay in order to maximize the chance of being selected from the mempool by a miner, the sender typically takes into account several factors, including the size of the transaction and the amount of transaction activity on the network. Instead of calculating the fee amount themselves, senders can also rely on their wallets’ dynamic fee structure, a feature of some wallets that monitors network volume and calculates the optimal fee for a given transaction.

---


179 An Ethereum Request for Comment (ERC) is a request by Ethereum developers for input from the Ethereum community. ERC Number 20 (ERC20) refers to a set of uniform standards for tokens issued on the Ethereum blockchain. ERC20 allows developers to design DApps without having to worry about rewriting the entire program each time a new token is issued.

180 To make an offline transaction using MEW, a user accesses the MEW program on an offline computer and inputs information for a transaction (i.e., the sender and recipient addresses, the amount, the gas limit, and the wallet information). The MEW program then generates a signed transaction, which the user can copy and paste to the user’s online computer for broadcasting to the Ethereum network. See Antonio Madeira, How to Use MyEtherWallet, CryptoCompare (Jun. 29, 2018), https://www.cryptocompare.com/wallets/guides/how-to-use-myetherwallet/.

181 Transactions that are included on a block are considered “confirmed.”


184 Id.

185 Id.

186 Id.

2.5.2 The Ethereum Network

On the Ethereum network, “gas” is the unit used for paying transaction fees. Unlike the Bitcoin network, where fees are voluntary and based on the size of the transaction, fees on the Ethereum network are mandatory, and the amount of fees actually paid (in Ether) is a function of the amount of computational work performed to verify the transaction.

In broadcasting the transaction to miners for verification, however, a sender cannot know the exact amount of work required to verify the transaction. There is always uncertainty because events can occur between transmission and mining that may affect the amount of computational resources required for verification, such as the mining of another block during the same period. In transmitting the transaction, therefore, the sender sets a transactional gas limit and gas price, in addition to including a certain amount of Ether. The transactional gas limit, sometimes called “start gas,” is the estimated amount of gas that the sender is willing to pay for the transaction. The gas price is the rate of Ether per gas that a user is willing to pay.

Miners decide which transaction to include on a block and often base this decision on gas price. Thus, if a user sets the gas price too low, miners may not pick the transaction for inclusion. Also, if insufficient Ether is sent, the transaction may never reach the miners or may “run out of gas”, resulting in a failed transaction. In that event, fees paid in the transaction go to the miner for performing work even if the transaction was not completed. If the amount of Ether sent exceeds the fee required to process the transaction, the excess is returned to the sender.

---

188 See Buterin, supra note 136.
189 Id.
190 Gas Limit * Gas Price = Fee Paid in Ether.
191 See Buterin, supra note 136.
192 Not to be confused with the block gas limit, which refers to the size of an Ethereum block. See infra Section 2.2.2.2.
193 See Buterin, supra note 136.
194 Id.
196 Id.
197 Id.
198 Id.
199 Id.
2.6 Exchanges

2.6.1 Centralized Exchanges

A virtual currency exchange is essentially a marketplace to exchange virtual currencies for fiat currencies (e.g., bitcoin to dollars) or for other virtual currencies (e.g., bitcoin to ether).\textsuperscript{200} Depending on the exchange, certain types of virtual currencies and fiat currencies may be exchanged on a platform.\textsuperscript{201} For example, Coinbase allows users to purchase certain virtual currencies, including bitcoin, Ether, and Litecoin, in exchange for dollars and euros.\textsuperscript{202} It also allows users to trade those virtual currencies for each other.\textsuperscript{203} Similarly, Gemini allows users to buy and sell bitcoin for dollars, and to buy and sell Ether for dollars and bitcoin.\textsuperscript{204}

Centralized virtual currency exchanges, such as Coinbase and Gemini, have a central authority or operator, who can control the platform by exercising powers like freezing all transaction activity or suspending user accounts.\textsuperscript{205} Before initiating transactions on an exchange, users are required to open an account with the operator, which may require information such as name, birthdate, and address, as well as copies of government-issued identification and utility bills.\textsuperscript{206} Centralized exchanges offer various advanced functions, such as allowing users to place buy/sell orders and conduct margin trading.\textsuperscript{207}

Many countries require centralized exchanges to comply with anti-money laundering (AML) and know-your-customer (KYC) regulations.\textsuperscript{208} In the United States, exchanges are required to register as money service businesses with the Financial Crimes Enforcement Network (FinCEN), and to comply with FinCEN regulations, including customer identification and


\textsuperscript{201} Id.


\textsuperscript{205} See Coinbase User Agreement, supra note 202.

\textsuperscript{206} Id.

\textsuperscript{207} Id.

\textsuperscript{208} See Chapter 6.
suspicious activity reporting requirements. Additionally, depending on the services offered, exchanges may need to obtain a license to operate as a money transmitter in most states.

2.6.2 Decentralized Exchanges

Decentralized exchanges, such as Bitsquare, are marketplaces with no central authority. Instead, trading takes place directly between users, peer to peer. Decentralized exchanges may operate through the use of proxy tokens (to represent fiat or virtual currency) or via an escrow system.

Unlike centralized exchanges, which must maintain servers and thus are susceptible to attacks, decentralized exchanges operate through distributed nodes on a network with no single point of failure. Additionally, decentralized exchanges do not require registration and do not store user information, thereby safeguarding user privacy.

---


214 Id.


216 See Madera, supra note 213.

To incentivize users to transact honestly, some decentralized exchange require security deposits and third-party arbiters. If one party to a transaction fails to perform, by failing to transfer an agreed upon amount of virtual currency, for example, then the aggrieved party may submit evidence to the arbiter that the aggrieved party did perform whereas while the breaching party failed to transfer the virtual currency. If the aggrieved party prevails, then the arbiter can sign the multi-signature wallet that holds the deposit, releasing it to the aggrieved party.

### 2.7 Virtual Currency ATMs

Virtual currency ATMs are kiosks that allow users to exchange virtual currency for fiat currency. Variations and functionalities of ATMs vary greatly between manufacturers and models. Some machines offer only one-way exchanges, selling virtual currencies to users in exchange for a cash deposit. Others have capacity for two-way exchanges, selling virtual currency to users for a cash deposit, or buying users’ virtual currency and dispensing fiat currency. ATMs also vary in terms of what virtual currencies they can support: some support bitcoin only, while others support many different coins, including Ether, Litecoin, and Dogecoin. ATMs can also be customized to satisfy AML and KYC regulations, by requiring names and addresses of users, or through the use of ID scanners and fingerprint readers.

To purchase virtual currency at an ATM, users must generally have a wallet address, which they can create beforehand or at the ATM. Each user’s identity is verified, either onsite by the ATM operator or by the ATM itself, which may require such information as the user’s name, address, phone number, ID, or palm print. Users then enter their wallet information, or scan

---


220 *Id.*


227 *Id.*
their wallet’s QR code, and insert cash into the machine. For each transaction, the ATM will show a listed price for the virtual currency, which is based on the exchange rate from various virtual currency exchanges. Once the transaction is confirmed, the ATM will transfer the virtual currencies to the user’s wallet.

The process of selling virtual currency through an ATM is similar to purchasing. Once the user’s identification is verified, the ATM will show a QR code that allows the user to scan and transfer the user’s virtual currency. The ATM will then dispense cash.

2.8 Executable Distributed Code Contracts

The ability to run an executable distributed code contract (EDCC) – typically, yet erroneously, referred to as a “smart” contract – is one of the main features of Ethereum. EDCCs are built upon the Ethereum blockchain as cryptographic “boxes” that contain value and only unlock if certain conditions are met, thereby enabling parties to formally specify a cryptographically enforceable agreement. EDCCs are computer programs that receive certain inputs, and perform according to a set of instructions.

The concept of EDCCs was first proposed in the 1990s, but the Ethereum network was the first to implement it on a decentralized distributed platform that enforced the terms and conditions. Ethereum has effectively synthesized law and economics with cryptography in the online world by allowing its users to embed many types of contractual clauses into computer software, the breach of which results in immediate enforcement. Therefore, EDCCs may be authored in order to algorithmically specify and autonomously enforce rules of interaction.

228 Id.
229 Id.
230 Id.
231 Id.
232 Id.
233 Id.
236 See Buterin, supra note 136.
237 For example, if a car has EDCC embedded into its control system, and the owner fails to make payments, the EDCC can immediately return control of the car to the bank. Id.
Despite the efficiencies and cost reductions created by EDCCs, they have been criticized as too rigid to adjust to changing circumstances because, once an EDCC goes live, it is unalterable and operates automatically according to its code.

2.9 Decentralized Applications

Decentralized applications (known as “DApps”) are software programs that operate on a decentralized network and share certain characteristics: 1) They are open source, requiring agreement from a majority of the users to make any changes; 2) their data is stored on a public blockchain; and 3) they use a cryptographic token issued according to a standard algorithm.

DApps can vary structurally and fall into one of three types. The first, Type I, has its own blockchain, such as Ethereum or Bitcoin. Type II uses a Type I blockchain but integrates its own protocols and tokens to function. Examples include Steemit, a social media site, and Augur, a prediction market – both of which use the Ethereum blockchain. Type III leverages the protocol of a Type II DApp but uses its own tokens to function. For example, the SAFE network uses the Omni Protocol for issuing the network’s own “safecoins,” which are used to obtain distributed file storage.

2.10 Decentralized Autonomous Organizations

A decentralized autonomous organization (known as a “DAO”) is an entity that “lives on the Internet and exists autonomously, but also heavily relies on hiring individuals to perform

239 Kristen Silverberg et al., Getting Smart: Contracts on the Blockchain, Institute of International Finance (May 2016), https://www.iif.com/Publications/ID/582/Getting-Smart-Contracts-on-the-Blockchain.


242 Id.


244 Id.


246 The term “DAO” should not be confused with “The DAO,” which was the name of a specific decentralized autonomous venture capital fund in which investors controlled the corporate governance of the organization by voting through the use of so-called “DAO tokens.”
certain tasks that the automaton itself cannot do.” It is a “virtual entity that has a certain set of members or shareholders which, perhaps with a 67% majority, have the right to spend the entity's funds and modify its code.”

A DAO is not like a traditional corporation or partnership, which has written bylaws or articles, and which are managed by actual people (e.g., board of directors, officers, managers, employees). Instead, DAOs exist entirely on a blockchain, and their operations are governed by EDCCs. A DAO may be structured to have varying degrees of human involvement. For some, governance may be automatic; in others, members may vote on governance issues (e.g., voting to change the DAO’s code, or on proposals made by other members) through the use of the DAO’s tokens.

Currently, a DAO is not recognized as a legal entity, creating uncertainty over liability issues such as whether the members, developers, or DAO itself bears legal responsibility for any misconduct.

247 See Buterin, supra note 238.
248 Id.
249 Id.
Chapter 3
3 Threats to Blockchain Networks

3.1 Cyberattacks

Cyberattacks – attacks that threaten the operation or use of a computer or computer system\(^\text{251}\) – have become increasingly common over the last few decades.\(^\text{252}\) They pose a particular risk to blockchain networks, which rely on computer software and the global interconnectivity of the Internet to operate. Blockchain networks, such as Bitcoin and Ethereum, are susceptible to cyberattacks and face unique threats due to the decentralized P2P network infrastructure inherent in each system. Virtual currency users should be aware of the various forms of cyberattacks to protect themselves against potential loss from service disruptions, privacy breaches, and thefts of virtual assets.

Blockchain-based businesses must also take precautions against cyberattacks, which can cause, *inter alia*, financial loss, loss of customers, loss of company or customer data, cost of recovery, and loss of reputation.\(^\text{253}\) While defenses and solutions are available in the event of cyberattacks, taking preventive measures to eliminate the risk of them altogether is the better practice, where possible.

3.1.1 Social Engineering

Social engineering, in the context of information security, refers to the psychological manipulation of individuals into performing desired actions or divulging confidential information.\(^\text{254}\) It is essentially a confidence trick performed to gather information, commit fraud, or gain system access, but differs from a traditional “con” in that it is often just one step within a more complex fraud scheme.\(^\text{255}\)

A recent example of a social engineering hack affecting blockchain users is the phone network hack.\(^\text{256}\) In several instances, hackers stole millions of dollars in bitcoin by analyzing


\(^{255}\) Id.

victims’ social media trends and emails to derive the passwords to their cell phone accounts.257 Hackers then contacted the victims’ cell phone providers to have their phone numbers ported to new providers of the hackers’ choice.258

Once a hacker controls a victim’s phone number, the hacker can request updated passwords for many security sites, such as Google, iCloud, DropBox and Evernote, some of which may contain the victim’s private keys for hot wallets.259 The hacker then uses the private key to transfer cryptocurrency from the user’s wallet into the hacker’s untraceable wallet.260 Given the nature of blockchain technology, these transactions cannot be reversed or traced to the hacker.261

3.1.2 Phishing

Phishing is a malicious attempt to obtain sensitive information, such as private keys, by masquerading as a trustworthy entity in an electronic communication.262 These attacks usually take the form of unsolicited phone calls or email messages.263 With respect to cryptocurrency stored on exchanges or in wallets, users should always keep sensitive information like their private keys and website passwords confidential, never disclosing it to anyone for any reason. Users should be particularly suspicious of unsolicited emails, phone calls, or text messages seeking sensitive information. Many email services and Web browsers offer an additional layer of security in the form of anti-phishing software, substantially reducing the threat of such attacks.264 South Korea reports that the 2017 hacks of Youbit were the result of phishing emails being sent to and opened by Youbit employees on their personal computers.265 The South Korean government alleges that the emails originated from North Korean IP addresses.266

257 Id.
258 Id.
259 Id.
260 Id.
266 Id.
3.1.3 Denial-of-Service

A Denial-of-Service (DoS) attack is a common cyberattack that causes loss of service to a computer or network of computers.\(^{267}\) By crippling network performance, it prevents legitimate users from accessing information or services.\(^{268}\) The most common form of DoS attack involves flooding the network with bogus information or requests, thereby crowding out legitimate network traffic.\(^{269}\) Another method is to drown the network in disproportionate computation, leaving it with insufficient power to address queries from legitimate users.\(^{270}\) Both types of DoS attacks create a bottleneck in the central server of the targeted program, substantially slowing down the network or even disabling it entirely.\(^{271}\)

A DoS attack causes systems to crash and potentially damages data stored on the server.\(^{272}\) Many attackers, especially those unskilled in computer programming, choose this type of cyberattack because it is relatively simple compared to the alternatives.\(^{273}\) DoS attacks can occur internally and are especially popular with disgruntled employees seeking to cause damage to their companies.\(^{274}\)

DoS attacks are more common in centralized Internet services, which use a central server for processing requests, rather than a decentralized P2P network, because a central server is easier to overload.\(^{275}\) Many virtual currency exchanges have experienced DoS attacks because their centralized servers are ripe targets for disruption. In 2014, for example, cryptocurrency exchanges Mt. Gox and Bitstamp had to freeze customer withdrawals due to inconsistent transaction confirmations caused by DoS attacks.\(^{276}\) DoS attacks have been less prevalent on exchange sites in more recent years, likely due to increased bandwidths and cyber security, and also to the growing preference among hackers for the more successful Distributed Denial-of-Service (DDoS) attacks described below.


\(^{268}\) U.S. Computer Emergency Readiness Team, *supra* note 263.

\(^{269}\) Pretre, *supra* note 267.

\(^{270}\) *Id.*

\(^{271}\) *Id.*

\(^{272}\) *Id.*

\(^{273}\) Stephenson, *supra* note 251 at 45.

\(^{274}\) *Id.*

\(^{275}\) Pretre, *supra* note 267.

DoS attacks are not always apparent and can be difficult to distinguish from common network activity. There is no general way to block a DoS attack, and the actual target or source of the attack is often difficult to decipher.277

3.1.4 Distributed Denial-of-Service

A DDoS attack is a more efficient form of DoS attack, allowing multiple hosts or computers to attack the network simultaneously, thereby amplifying the attack’s effects.278 The attackers perpetrating a DDoS attack use not just their own computer (or network of computers) but also other computers connected to the Internet.279 The attackers infect the remote computers with a virus or Trojan Horse, turning them into so-called “zombies” and giving hackers complete control over the computer’s function and processing power.280 In comparison to a DoS attack, it is even more difficult to determine the target or source of a DDoS attack due to its distributed nature and the fact that such attacks are launched by multiple computers – all with different IP addresses.281

The Ethereum network faced a massive DDoS attack in September and October 2016, resulting in delayed block validation.282 The attacker used an operation code called “Extcodesize,” which flooded the network with transaction requests, causing blocks to take as long as 60 seconds to validate283 instead of the usual 15 seconds.284 The Ethereum mining community remedied the situation by implementing several hard forks to change the protocol, update the gas limit, and add state journaling – all of which eventually addressed the root of the DDoS exploit.285

3.1.5 Malware

Malware is rogue or malicious source code.286 A malware attack is facilitated through computer software and used for illicit activities like data exfiltration, DoS attacks, fraud, and spam dissemination.287 While centralized infrastructures are often susceptible to a single point of failure

277 U.S. Computer Emergency Readiness Team, supra note 263.
278 Id.
279 Id.
280 Pretre, supra note 267.
281 Id.
285 Meegan, supra note 282.
286 Stephenson, supra note 273.
287 Id.
due to malicious attacks, the decentralized nature of blockchain technology makes malware attacks on blockchains unlikely.

However, cryptocurrency users are not immune to such attacks since private keys and passwords stored on computers connected to the Internet are still susceptible. In 2016, Russian Internet security research center Kaspersky Labs reported that 31.9% of computers had experienced at least one malware attack over the past year, and that malware targeting cryptocurrencies increased 11-fold between January and September 2016.

### 3.1.5.1 Viruses, Trojan Horses and Worms

The three most common types of malware are viruses, Trojan Horses, and worms. A virus is a type of malware that has two distinguishing characteristics. First, the virus code is written to replicate itself. Second, the virus must become part of another executable file in order to survive. Some viruses can permanently destroy files and shut down a computer, while others cause only minimal disruption to the computer’s normal operations. Infection can occur when a user downloads the virus from a webpage, email attachment, or other source. The virus then infects an executable program or application. Once that program or application is run by the user, control is transferred to the virus, which replicates itself throughout the host computer, potentially spreading to other computers, too.

A Trojan Horse is a type of malware designed to steal online account credentials by masquerading as a different, more credible program. It differs from a virus in that it does not

---


290 Stephenson, *supra* note 251.

291 Id.

292 Id.


295 Id.

296 Id.

replicate or infect other files and can stand on its own as an executable file.\textsuperscript{298} One type of Trojan Horse is a program that steals user passwords and forwards them to the attacker.\textsuperscript{299} In such cases, the malware is either embedded in legitimate source code, making it difficult to discover, or maliciously introduced by replacing critical files with those containing the Trojan Horse.\textsuperscript{300} Once the attack succeeds, the attacker can enter the system undetected, collect information, open back doors for others to enter undetected, create unauthorized accounts, and gain superior rights to the program.\textsuperscript{301}

Worms are similar to viruses but cannot replicate themselves within other programs.\textsuperscript{302} Instead, the worm duplicates itself as a stand-alone program and disrupts the functionality of the computer by consuming excessive amounts of disk space, processing power, memory, and other computer resources.\textsuperscript{303} Worms pose a particular threat to P2P networks because such networks are composed of computers that all run the same software, allowing the worm to spread easily.\textsuperscript{304} Also, P2P networks routinely handle large files, permitting attackers to deploy worms with complex behaviors and no concern for size.\textsuperscript{305} An attacker can compromise an entire network just by finding one exploitable security hole.\textsuperscript{306}

Such malware attacks can be mitigated by anti-virus software, which removes malicious code already on a computer, and enables a firewall on the users’ broadband Internet connection that blocks malicious code from infiltrating the computer in the first place.\textsuperscript{307} While the decentralization of a P2P network makes it difficult to execute malware, Interpol has created proof-of-concept software demonstrating how malware can take information from a hacker-controlled Bitcoin address and a transaction hash over a command line.\textsuperscript{308} This demo malware connects to the Bitcoin network, requests certain blockchain data from a Bitcoin address containing potentially malicious information, locates the related transaction, extracts sections of code, then runs the sections as one.\textsuperscript{309} This maneuver bypasses the decentralized protection of the network and

\begin{footnotes}
\textsuperscript{298} Id.
\textsuperscript{299} Id.
\textsuperscript{300} Id.
\textsuperscript{301} Stephenson, supra note 251, at 50.
\textsuperscript{302} Id.
\textsuperscript{303} Pretre, supra note 267, at 8-9.
\textsuperscript{304} Id.
\textsuperscript{305} Id.
\textsuperscript{306} Id.
\textsuperscript{307} Stephenson, supra note 251, at 50.
\textsuperscript{309} Thomas Fox-Brewster, Bitcoin’s Blockchain Offers Safe Haven for Malware and Child Abuse, Warns Interpol, Forbes (Mar. 27, 2015),
\end{footnotes}
operates similarly to torrent files, compiling small sections of malicious code contained within individual addresses.  

It is unlikely that developers will ever be able to write source code that is guaranteed to be invulnerable, especially over a malleable P2P network; however, steps are being taken to create anti-virus protection powerful enough to rival any realistic malware threat.

3.1.5.2 Botnet

Botnets are the primary source of online crime and arguably one of the greatest threats to the Internet infrastructure. Botnet is short for “robot network,” a network of automated computers, including mobile devices, which can be controlled or updated remotely by one of many sources. Botnets are typically embedded in Trojan Horse malware. The malware compromises a computer and merges into a botnet, which can then be used to perform DoS attacks, send spam e-mail, host illegal content, or aid in most other types of online criminal behavior.

Botnets have also been used to mine cryptocurrency. Between September 2013 and early spring 2014, hackers gained administrative access to Taiwanese corporation Synology and illegally mined cryptocurrency using thousands of computers owned by Synology’s customers.

3.1.5.3 Sybil Attack

A Sybil attack subverts the reputation system of a P2P network by presenting false identities in the network. A single computer presents thousands of identities that are seemingly distinguishable from each other – e.g., by creating thousands of fake users on a blockchain all with unique addresses – and gains control over part of a network through a false-user monopoly.


310 Id.


315 Id.


318 Id.
Such an attack can disable a botnet by presenting enough identities to dominate a network.\textsuperscript{319} For example, if a botnet comprises 50% of users on a network, then a Sybil attack can be used to increase the total number of users by presenting false identities, thus decreasing the botnet’s 50% control to a lower percentage. A Sybil attack is difficult to execute because it takes a significant amount of computing power to run so many false identities; however, there are no mechanisms that can completely prevent such an attack.\textsuperscript{320} The Sybil attack is thus one of the greatest challenges faced by businesses that operate on the Internet.\textsuperscript{321}

While there is no way to completely prevent a Sybil attack, defenses do exist. Centralized Internet services with trusted certifications, such as Gmail, often require users to provide a phone number to verify the creation of a new account to determine whether the user is human.\textsuperscript{322} Another feature many centralized services use as a form of resources testing is the Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA).\textsuperscript{323} This is a challenge-response test that requires new users, and often users who are changing their passwords, to type a pre-generated word or describe a pre-generated image in order to verify that the user is human and not some forged identity.\textsuperscript{324}

The public-private key cryptography used by purely distributed blockchain networks, like Bitcoin and Ethereum, can eliminate this type of attack.\textsuperscript{325} These networks rely on miners to validate transactions and issue new currency. A Sybil attack could be used by a malicious actor running multiple counterfeit identities at the same time, which could allow them to control the network through a so-called “51% attack,” described below.\textsuperscript{326} However, it is unlikely they would be able to achieve the necessary hashing power to perform a Sybil attack in this manner. The implementation of public-private key cryptography has been shown to lessen this threat due to the

\begin{quote}
\textsuperscript{319} Adam Louis Verigin, \textit{Evaluating the Effectiveness of Sybil Attacks Against Peer-to-Peer Botnets}, University of Victoria (2013),
\textsuperscript{321} \textit{Id}.
\textsuperscript{322} Baptiste Pretre, \textit{Attacks on Peer-to-Peer Networks} (2005), Swiss Federal Institute of Technology Zurich, Section 3.3.1 – Worm Propagation,
\texttt{http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.447.7128&rep=rep1&type=pdf}.
\textsuperscript{324} \textit{Id}.
\textsuperscript{326} \textit{See infra} Section 3.1.7.
\end{quote}
requirement that all users individually authenticate themselves, causing duplicates to be easily discovered and eliminated.

3.1.5.4 Ransomware

Ransomware is covertly installed malware designed either to prevent normal use of a personal computer by locking down access, or rendering the documents and files on a computer inaccessible by encrypting them.\textsuperscript{327} Once the computer is infected, a ransom demand is then displayed, usually either in a text file or as a webpage in a browser, requesting payment in exchange for restoring access to the computer or decrypting the documents and files.\textsuperscript{328} In 2017, the average ransom demand was $522.\textsuperscript{329}

A user may be exposed to a ransomware threat in a variety of ways, such as by visiting a malicious or compromised website that hosts exploit kits,\textsuperscript{330} as a byproduct of another type of malware, or as an attachment to a spammed email.\textsuperscript{331} Ransomware is a lucrative revenue channel, and many malware authors continually improve their malware to better target their victims.\textsuperscript{332} Some ransomware creators even sell their ransomware to other cybercriminals, who then operate ransomware attacks and share their profits with the creator.\textsuperscript{333}

Ransomware has grown considerably since the advent of bitcoin, which has provided a payment method that, unlike PayPal or credit card transactions, is largely untraceable. Use of the ransomware program “CTB-Locker,” in particular, has been growing since early 2016. This malware encrypts a website through DDoS attacks, then demands that the owner transfer bitcoin to a specified bitcoin address.\textsuperscript{334} Hackers ensure anonymity by creating a separate bitcoin wallet with a unique address for each website they encrypt, which they then publish on the site.\textsuperscript{335}

\textsuperscript{328} \textit{Id}.
\textsuperscript{330} Exploit kits gather information on the victim machine, find vulnerabilities and determine the appropriate exploit, which then silently downloads and executes the malware.
\textsuperscript{333} \textit{Id}.
\textsuperscript{335} \textit{Id}. 
In May 2017, the largest ransomware attack occurred across the globe, infecting 300,000 computers in 150 different countries. The attack encrypted files on PC hard drives, making the data impossible to access, and then demanded payment of $300-600 in bitcoin to retrieve the data. The countries most affected by the attack were Russia, where the Interior Ministry was hit, Taiwan, Ukraine and India. The attack struck several important and high-profile systems in other countries, including Britain’s National Health Service. The hackers used “WannaCry” ransomware, which was delivered as an email and exploited a vulnerability in Windows operating systems. In March 2017, before the rapid spread of the attack, Microsoft had released Microsoft Security Bulletin MS17-010 and a patch to prevent such vulnerabilities. Yet, despite Microsoft flagging the patch as critical, many systems remained unpatched when the attacks began.

As those infected by the WannaCry ransomware can attest, restoring a computer after a ransomware attack can be very difficult, and payment of the ransom does not guarantee that access to the computer or server will be regained. To avoid being compromised by such an attack, it is recommended that users regularly back up files and data, ensure that security software is up to date, use a strong firewall, and enable a popup blocker. Finally, since most ransomware is poorly coded, or master keys leak, some experts suggest looking online for a verified decryptor tool to decrypt the impacted data.

### 3.1.6 Replay Attack

A replay attack occurs when an unauthorized user captures network traffic then sends the communication to its original destination, acting as the original sender. For example, the victim

---


337 Id.


339 Id.


342 Id.

343 Pathak, *supra* note 331.


sends a message to a server, and a hacker intercepts and forwards this message to the server as if
the hacker were the original sender. A replay attack on a blockchain could allow a hacker to take
one legitimate transaction on one blockchain and then fraudulently repeat it on another.346 Replay
attacks can be eliminated on blockchain technology by using different addresses and keys between
different chains, with different identifiers such as “prefixes.”347 Authentication systems like
timestamps, sequence numbers, or session IDs can prevent this type of attack from succeeding.

3.1.7 51% Attack

A so-called “51% attack,” also known as a “cartel of miners attack,” is a potential risk to
any cryptocurrency blockchain. The security of blockchain technology relies on the distributed
consensus achieved by mining. A 51% attack could occur if a cartel of minors colludes to achieve
more than 50% of all hashing power, giving them majority control over the voting process, and
allowing them to out-compute any other chain.348

If such an attack succeeds, the cartel could refuse to acknowledge any blocks besides its
own as valid, thus preventing anyone else from mining and collecting the block reward.349
Alternatively, the entity could censor the network by refusing to include certain historical
transactions.350 Censorship is accomplished when the entity goes “back in time” to a previous
block and mines from there, creating a fork in the blockchain that results in two parallel chains
existing simultaneously.351 The new chain will inevitably overtake the original chain once the
mining on the former becomes more difficult and profitable.352 Miners will allocate their resources
to the more difficult chain, negating the effect of any transactions that took place in the original
chain after the fork point.353

If a cartel of miners ever achieved a 51% attack and controlled the majority of the hashing
power in a network, they could reverse their own transactions, which would allow for double-
spending.354 The miners could also prevent some or all new transactions from gaining any

346 J.P. Buntinx, What is a Bitcoin Replay Attack?, The Merkle (Mar. 22, 2017),
https://themerkle.com/what-is-a-bitcoin-replay-attack/.
347 Steve Marx, Signing and Verifying Messages in Ethereum, Program the Blockchain (Feb. 17,
ethereum/.
348 Vitalik Buterin, Bitcoin Magazine: On Mining (Jun. 20, 2014),
349 Id.
350 Id.
351 Id.
352 Id.
353 Id.
354 Burgess Powell, Not Only is a 51% Attack on Blockchain Possible, But It’s Coming, Blocklr
However, the miners would not be able to change the number of coins generated per block or per block reward. Nor would they be able to assign themselves an arbitrary number of coins or steal any other user’s coins. The only way a cartel could do either of these things would be if they reversed a transaction, which the design of blockchain makes computationally infeasible.

While large mining pools exist, none are remotely close to controlling 51% of the Bitcoin network, where the largest mining pool controls 17.5%, or the Ethereum network, where the largest mining pool controls approximately 26.1%. Moreover, it is unlikely that miners would participate in a pool with the goal of executing a 51% attack because doing so would likely collapse the value of the cryptocurrency attacked and bankrupt the miners themselves. As miners rely on the block reward to fund their operations and earn profits, there is no incentive for them to participate in an attack that would likely render those block rewards worthless.

Additionally, it is much more difficult to change historical blocks, and doing so becomes exponentially more difficult the further back one goes. Even if successful, changing historical blocks would only allow the attacker to censor and change the ordering of the transactions. Checkpoints in the blockchain, which prevent reorganization past a specified block, are also used to militate against this type of attack.

If and when Ethereum successfully transitions to a system of Proof-of-Stake mining, computational power and hash rate will no longer be the controlling factors for a 51% attack. Instead, an attacker would need to obtain over 51% of all Ether in existence to achieve controlling power. This would be prohibitively costly and difficult considering that, as of November 2018, there are roughly 103,000,000 Ether in circulation.

355 Buterin, supra note 348.
356 Id.
357 Id.
360 See Etherchain.org, Mining Statistics (Last 24h), https://www.etherchain.org/charts/topMiners (last visited Nov. 6, 2018).
361 Buterin, supra note 348.
362 Id.
363 BitcoinWiki, supra note 358.
364 Id.
3.1.8 Variations on the 51% Attack

3.1.8.1 Goldfinger Attack

A Goldfinger attack utilizes the same strategy as a 51% attack, but its sole purpose is to destroy the cryptocurrency economy in order to further some goal outside of the blockchain. As discussed above, a successful 51% attack would likely cause a cryptocurrency’s value to plummet, rendering such an attack generally unprofitable. Even so, a Goldfinger attack has many potential non-pecuniary motivations. For example, a government or institution might want to block cryptocurrency transactions to enforce the law, deter money laundering, or achieve some other institutional goal. Alternatively, a non-state attacker might seek to accomplish some political or social goal – e.g., as a form of social protest.

Given the computer processing power required to effectuate a Goldfinger attack, governments are more likely candidates to launch them than private actors. For example, a government could possibly initiate such an attack as a law enforcement tactic to manage illegal activity or prevent repeats of the infamous Silk Road scandal. Indeed, given that traditional law enforcement is ill-suited to police blockchain technology, and there is no central issuing authority or direct means of identifying the parties involved in transactions, some governments may resort to such tactics to prevent these networks from being used for criminal activity.

3.1.8.2 Feather Forking

A so-called “feather forking” or “block discouragement” attack yields similar results to a 51% attack but without the requirement of 51% of miners for execution. Feather forking begins when a single miner tries to censor a set of target transactions by publicly promising that, if a targeted transaction is included in the blockchain, the miner will retaliate by ignoring the block and attempting to cause a fork. Whereas honest miners will build on any valid block, regardless of its contents, a malicious miner engaged in feather forking will refuse to build on any chain containing the undesired block. The attacker creates a new fork that will continue until it either


367 Id.

368 Such a model was previously postulated under the name of “Occupy Bitcoin.” J. Becker et al., *Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency*, Workshop on the Economic of Information Security WEIS (2012).


372 Id.

373 Id.
successfully outraces the original chain or falls behind, causing the attacker to concede, continue mining the longer original chain, and accept the publication of the targeted transaction.\footnote{374} 

The probability of a successful attack for a solo miner is very low considering their low hashing power and the likelihood that another miner, with virtuous intentions, will mine the targeted block. A feather fork only becomes a realistic threat when a group of miners collude to blacklist the transaction.\footnote{375} Failure means a considerable waste of mining effort, substantially reducing the miner’s revenues.\footnote{376} For such a threat to be credible, therefore, the attacker must first demonstrate not just willingness to undertake the attack but the ability to commit the requisite resources as well.\footnote{377} The attacker can do so by successfully carrying out an attack then using it as a proof to entice collusion.

Most miners do not discriminate between valid blocks. Even so, it is plausible that, in the future, mining pools may distinguish themselves by earning more profit and running so-called “greedy code,” which would give them incentive to follow through with the feather fork. An attacker can enforce a blacklist by threatening that, unless other miners join the attack, the attacker will retaliate by causing a costly feather fork. The attack thus resembles the Chicken game from game theory,\footnote{378} wherein players have an incentive to convince their competitors that they will do something self-destructive if the others do not yield.

\subsection*{3.1.8.3. Eclipse}

An eclipse attack allows the hacker to gain sufficient power to manipulate the blockchain, yielding the same rewards as a 51\% attack but without the majoritarian requirement for mining hashrate.\footnote{379} The decentralized network on a blockchain allows adversarial nodes to join and monopolize the victim’s incoming and outgoing connections, isolating that victim from all other peers in the network.\footnote{380} The attacker can control and filter the view of the blockchain from the victim’s perspective, forcing the victim to either waste computation power or allow the attacker to co-opt the victim’s compute power for malicious purposes.\footnote{381}

\footnotetext[374]{Id.}


\footnotetext[376]{Andrew Kim et al., The Stateless Currency and the State: An Examination of the Feasibility of a State Attack on Bitcoin (May 13, 2014).}

\footnotetext[377]{Bonneau, supra note 371.}


\footnotetext[380]{Id.}

In an eclipse attack, the attacker controls nodes by rapidly and repeatedly forming unsolicited incoming connections from attacker-controlled IP addresses, which are used to send false network information to victims.\textsuperscript{382} When a victim restarts and establishes the P2P network, there is a high probability that outgoing connections will actually be to the IP addresses controlled by the attacker.\textsuperscript{383} The attacker can then use this position to take over the victim’s hashing power, enhancing the attacker’s own power to manipulate the blockchain’s ledger in proportion to the number of victims and total hashing power seized.\textsuperscript{384}

The main barrier to an eclipse attack is the requirement that the attacker monopolize a considerable number of IP addresses.\textsuperscript{385} This is difficult for a solo attacker to accomplish without utilizing a botnet. A state actor or large company controlling many IP addresses might plausibly attack the infrastructure of a blockchain network.\textsuperscript{386} The attack could also be used to engineer block races by hoarding blocks discovered by eclipsed miners then releasing the blocks back to eclipsed and non-eclipsed miners alike once a competing block has been found.\textsuperscript{387} This would cause the eclipsed miners to waste effort and processing power on orphan blocks.\textsuperscript{388}

The eclipse attack also makes it more technically feasible to complete a 51% attack by lowering the minimum hashing rate as the attacker gains control over more and more eclipsed miners.\textsuperscript{389} While this could help facilitate a 51% attack, it would still result in catastrophic devaluation of the cryptocurrency, so the likelihood of such an attack remains remote.

### 3.1.9 Selfish Mining

A selfish-mine allows a mining pool of sufficient size to obtain revenue larger than its ratio of processing power.\textsuperscript{390} The selfish-mining pool keeps its discovered blocks private, secretly forking the blockchain and creating a private branch.\textsuperscript{391} The honest miners working on the original chain continue mining, unaware that they are working on a shorter branch.\textsuperscript{392} Then the selfish-mining pool competes to find blocks before the honest pool, attempting to extend its new chain.\textsuperscript{393}

\textsuperscript{382} Id.
\textsuperscript{383} Id.
\textsuperscript{384} Id.
\textsuperscript{385} Id.
\textsuperscript{386} Id.
\textsuperscript{387} Id.
\textsuperscript{388} Id.
\textsuperscript{389} Id.
\textsuperscript{391} \textit{Japanese Cryptocurrency Monacoin Hit by Selfish Mining Attack}, CCN (May 21, 2018), \url{https://www.ccn.com/japanese-cryptocurrency-monacoin-hit-by-selfish-mining-attack/}.
\textsuperscript{392} Id.
\textsuperscript{393} Id.
Considering that the selfish-mining pool possesses only a small fraction of the network’s total hashing power, its private branch will not remain ahead of the original chain indefinitely.

Both the attacker and the honest miners waste energy, but the latter waste proportionately more, while the former gain rewards disproportionate to their share of the processing power. The selfish miners gain a competitive advantage, thus incentivizing profit-driven miners to join their version of the blockchain. This type of attack undermines the decentralized nature of the network by leading to a further consolidation of mining power in the hands of selfish-miners.

The selfish-mining pool would then reveal blocks from its private branch, which the honest miners would begin mining in lieu of the shorter public branch. This wastes any previous effort spent on the shorter public branch and enables the selfish-mining pool to collect higher revenues by incorporating a higher fraction of its blocks into the blockchain. However, the chances of selfish miners overtaking the main branch are small in view of their lower processing power. The selfish-mining pool would fall back onto the main branch whenever the private branch ultimately falls behind its public counterpart.

The chances of selfish-mining’s overtaking the main branch are substantially higher where the attackers have previously performed an eclipse attack. In that case, the ratio of mining power controlled by the attackers is far greater and thus more likely to overpower the honest miners, causing selfish mining to become a much easier exploit.

3.1.10 Finney Attack

The Finney attack has the effect of double-spending – i.e., allowing the same coins to be spent more than once. The attacker creates a transaction crediting one of its own addresses but does not broadcast it to the network. A second transaction is then created paying the same coins to the victim, typically a merchant, who merely checks its propagation in the network and accepts the transaction without confirmation.

---

394 Kim, supra note 376.
395 Eyal & Gün Sirer, supra note 390.
396 Id.
397 Id.
398 Id.
399 Id.
401 Id.
403 Id.
404 Id.
The Finney attack only works if the merchant accepts unconfirmed transactions, or if the merchant waits a few seconds before verifying that the network agrees that the merchant has been paid.\textsuperscript{405} The attacker keeps the proceeds of the first transaction while proceeding to mine the fraudulent transaction. The attacker then broadcasts the secretly mined block, which overrides the unconfirmed payment to the victim even if it is propagated through the whole network.\textsuperscript{406} This type of attack can be completed with significantly less than 50% of the network’s hashrate, but is very time-consuming and thus less desirable.\textsuperscript{407} The attacker must wait for a block to mine, then compete and risk losing the block. If that occurs, then the attacker loses the reward and must repeat the process.\textsuperscript{408}

This variant of the double-spend attack is undetectable until fully executed but very difficult to execute because mining a block solo is not been easy.\textsuperscript{409} The lower an attacker’s hashrate, the less opportunity that attacker has to carry out the attack. If the purpose is to obtain some type of illiquid good, it may be difficult to find a block when need for the good requires it. And if the purpose is to obtain something liquid – i.e., exchanging one cryptocurrency for another currency – the opportunity is ever-present but will likely require several transaction confirmations.\textsuperscript{410}

The only way for a merchant to protect against a Finney attack is to require at least one confirmation for a transaction before delivering purchased goods or cryptocurrency.\textsuperscript{411} Also, it is good practice to require additional confirmations, depending on the value of the goods or cryptocurrency being delivered.

\textsuperscript{405} Id.
\textsuperscript{406} Mong Yunheng et al., \textit{Design Weaknesses in the Bitcoin System}, Introduction to Information and System Security 57-63 (Jul. 2015), \url{http://www.comp.nus.edu.sg/~hugh/CS2107/Projects/Projects-CS2107-14-15-IV.pdf}.\textsuperscript{407} Cinerama, \textit{Risks of the Double Spending Attack}, Bitcoin Isle (Sept. 27, 2017), \url{https://www.bitcoinisle.com/2017/09/27/risks-of-the-double-spending-attack/}.\textsuperscript{408} Id.\textsuperscript{409} Mukherjee, \textit{supra} note 402.\textsuperscript{410} Id.\textsuperscript{411} Id.
Chapter 4

Current Virtual Currency and Blockchain Regulations and Legislative Efforts in the United States

4.1 Congressional Action Regarding Blockchain Technology and Virtual Currency

A decade after Satoshi Nakamoto introduced bitcoin, the U.S. government still has yet to provide a comprehensive regulatory framework for virtual currency and blockchain technology. Thus far, Congress has done little besides issuing a resolution, forming a legislative caucus, and passing a bill to provide for the assessment of the risks associated with blockchain technology.

4.1.1 H. Res. 835

Passed on September 12, 2016, House of Representatives Resolution 835 expressed the view that the United States should encourage the development of financial technology, including blockchain technology and non-fiat currencies. The resolution acknowledged that blockchain technology could substantially impact a wide range of industries and that virtual currencies could replace older payment options.412

The resolution further called for the United States to “prioritize accelerating the development of alternative technologies that support transparency, security, and authentication in a way that recognizes their benefits, allows for future innovation, and responsibly protects consumers’ personal information,” and to “support further innovation, and economic growth, and ensure cybersecurity, and the protection of consumer privacy[.].”413

While H. Res. 835 seemed to send a strong bi-partisan signal that the House recognized the importance of regulating blockchain technology and virtual currency, that chamber has yet to make this a priority in actual practice.

4.1.2 Congressional Blockchain Caucus

In February 2017, Reps. Jared Polis and David Schweikert relaunched the Congressional Blockchain Caucus,414 which focuses on advocating for “sound public policy toward Blockchain-based technologies and digital currencies.”415 According to Rep. Polis, “Blockchain’s potential to reshape everything from the financial industry to supply chains, to cybersecurity, to health care is something we should embrace.”416 The goal of the Congressional Blockchain Caucus is “to

413 Id.
415 Id.
416 Id.
educate, engage, and provide research to help policymakers implement smart regulatory approaches to the issues raised by blockchain-based technologies and networks.”

On September 21, 2018, Reps. Tom Emmer and Bill Foster were announced as co-chairmen of the Caucus, along with Reps. Polis and Schweikert. The Caucus’ initial areas of focus include government applications, data ownership, and healthcare.


Introduced on June 7, 2017, and sponsored by Rep. Mac Thornberry, House Bill 2810, The National Defense Authorization Act for Fiscal Year 2018 includes a requirement that the Secretary of Defense and other agencies report back to Congress on the potential offensive and defensive cyber capabilities of blockchain technology and other distributed database technologies. More specifically, the Department of Defense is to assess the use, planned use and vulnerabilities of blockchain technology in the United States. Many believe that Congress is seeking to determine the risks posed before it initiates any pilot programs based on distributed ledger technology. This Bill became law on December 12, 2017.

4.1.4 H.R. 3364 – Countering America’s Adversaries Through Sanctions Act

Introduced on July 24, 2017, and sponsored by a bipartisan group of representatives, House Bill 3364, the Countering America’s Adversaries Through Sanctions Act directs the President to sanction Iran, requires the President to submit for congressional review certain actions to terminate or waive sanctions against Russia, and modifies the President’s authority to sanction North Korea. The bill also requires the Secretary of Treasury to develop a national strategy to combat terrorist and other illicit financing, including the use of cryptocurrencies. The bill was enacted on August 2, 2017, after passing nearly unanimously in Congress (419 to 3 in the House, and 98 to 2 in the Senate).

417 Id.
419 Press Release, supra note 418.
422 Id.
4.1.5 Pending Federal Legislation

4.1.5.1 H.R. 4768 – National Strategy for Combating the Financing of Transnational Criminal Organizations Act

Introduced on January 1, 2018, and sponsored by Reps. David Kustoff, Kyrsten Sinema, Claudia Tenney, and Luke Messer, House Bill 4768, the National Strategy for Combating the Financing of Transnational Criminal Organizations Act, requires the President (via the Secretary of Treasury) to “develop a national strategy to combat the financial networks of transnational organized criminals” that must include a risk assessment related to the misuse of digital currencies.424

On March 6, 2018, the House passed the bill, and the next day it was received by the Senate and referred to the Committee on Banking, Housing, and Urban Affairs.425

4.1.5.2 H.R. 5036 – Financial Technology Protection Act

Introduced on February 15, 2018, and sponsored by Ted Budd, Kyrsten Sinema, and Stephen Lynch, the Financial Technology Protection Act intends to create an interagency task force dedicated to combating the illicit use of cryptocurrency for terrorist purposes.426 If enacted, the bill would create a fund to pay cash rewards of up to $450,000 to anyone who provides information leading to the conviction of “an individual involved with terrorist use of digital currencies.”427 The House passed the bill on September 26, 2018, and it was received by the Senate the next day.428

4.1.5.3 H.R. 6913 – Blockchain Promotion Act of 2018

Introduced on September 28, 2018, and sponsored by Reps. Brett Guthrie and Doris Matsui, House Bill 6913 seeks to create a Blockchain Working Group, which would within a year of the bill’s passage submit a report to Congress containing: (1) the recommended definition of blockchain technology; (2) a study on the impact of blockchain technology on ‘electromagnetic spectrum policy;’ and (3) a study and recommendations on how federal agencies can utilize blockchain technology.429

425 Id.
427 Id.
428 Id.
4.1.5.4 H. Res. 1102 – Expressing Support for Digital Currencies and Blockchain Technology

Introduced on September 28, 2018, and sponsored by Rep. Tom Emmer, House Resolution 1102\textsuperscript{430} proposes that Congress express support for cryptocurrency and blockchain technology in the following ways:

- Prioritize accelerating the development of blockchain technology to support transparency, security, and authentication in a way that recognizes its benefits and allows consumer protection while supporting future innovation;
- Create an environment that enables the American private sector to lead on blockchain innovation and further the growth and success of blockchain networks and digital currencies;
- Federal agencies should work toward a coordinated framework to support digital currencies and blockchain technology;
- Avoid undue restrictions on blockchain networks and the trustworthy decentralized computing services that they facilitate;
- Prevent and condemn illicit use of digital currencies and blockchain technology, and its aim should be to support and enforce a predictable, light-touch, consistent, and simple legal environment for services facilitated by blockchain networks; and
- Recognize the potential benefits and broad use of digital currencies and blockchain technology to enhance public services and enable more business growth, capital formation, and capital investment.\textsuperscript{431}

The Bill was referred to the Committee on Energy and Commerce and the Committee on Financial Services.

4.1.5.5 H.R. 6974 – The Blockchain Regulatory Certainty Act

Introduced on September 28, 2018, and sponsored by Rep. Tom Emmer, House Bill 6974 would prohibit both federal and state governments from treating blockchain developers or providers of blockchain services as money transmitters, money services businesses, financial institutions, or any other designation requiring a license or registration.\textsuperscript{432} The Act defines ‘Blockchain Developer’ as “any person or business that creates, maintains, or disseminates software facilitating the creation or maintenance of a blockchain network\textsuperscript{433} or a blockchain

\textsuperscript{430} H. Res. 1102, 115\textsuperscript{th} Cong. (2018) [https://www.congress.gov/bill/115th-congress/house-resolution/1102].

\textsuperscript{431} Id.


\textsuperscript{433} Pursuant to the bill, ‘Blockchain Network’ is defined as “any system of networked computers that cooperates to reach consensus over the state of a computer program that allows users to participate in the consensus-making process without the need to license proprietary software or obtain permission from any other user. The term includes, specifically, a public network of
The Bill was referred to the Committee on Financial Services and the Committee on the Judiciary.

4.1.5.6 H.R. 6973 – The Safe Harbor for Taxpayers with Forked Assets Act of 2018

Introduced on September 28, 2018, and sponsored by Rep. Tom Emmer, House Bill 6973 would provide a temporary safe harbor for the tax treatment of hard forks of convertible virtual currency in the absence of administrative guidance. The Bill was referred to the House Committee on Ways and Means.

4.1.6 Other Congressional Initiatives That May Ultimately Impact Blockchain Technology and Cryptocurrency

4.1.6.1 Congressional FinTech and Payments Caucus

In March 2015, the Congressional Payments Technology Caucus was formed to explore new and innovative technologies in the payments industry, and to focus on data security and access to electronic payments by the underserved. In December 2016, the Caucus changed its name to the Congressional FinTech and Payments Caucus to reflect the reality that new financial technology is changing the payments industry.

4.1.6.2 2018 Congressional Economic Report

The 2018 Congressional Economic Report, released by the U.S. Congress’ Joint Economic Committee, includes a chapter on blockchain technology and cryptocurrency. The committee recognized that, while 2017 was “the year of cryptocurrencies,” there are more uses for blockchain technology “as a potential tool for securing America’s digital infrastructure.” The chapter goes on to make the following recommendations:

__

computers that cooperates to reach consensus over the state of a distributed ledger describing transactions in a digital currency.”

Id.


Pursuant to the bill, ‘Hard Fork’ “means, with respect to any convertible virtual currency, any material change in the shared digital ledger which is used to verify by consensus transactions in such currency if such change results in the maintenance of independent shared digital ledgers with respect to such currency.”

Pursuant to the bill, ‘Convertible Virtual Currency’ “means any digital representation of value that (i) functions as a medium of exchange, a unit of account, or a store of value; (ii) does not have legal tender status; and (iii) has an ascertainable equivalent value in legal tender or is used as a substitute for legal tender.”


• “Policymakers and the public should become more familiar with digital currencies and other uses of blockchain technology, which have a wide range of applications in the future.”

440

• “Regulators should continue to coordinate among each other to guarantee coherent policy frameworks, definitions, and jurisdiction.”

441

• “Policymakers, regulators, and entrepreneurs should continue to work together to ensure developers can deploy these new blockchain technologies quickly, and in a manner that protects Americans from fraud, theft, and abuse, while ensuring compliance with relevant regulations.”

442

• “Government agencies at all levels should consider and examine new uses for this technology that could make the government more efficient in performing its functions.”

443

4.1.6.3 Other Congressional Caucuses Related to New Technologies

In addition to the Congressional Blockchain Caucus and the Congressional FinTech and Payments Caucus, members of the House of Representatives have also recently launched several other caucuses to explore and educate members about new technologies.

In January 2015, the Congressional Caucus on the Internet of Things (IoT) was established to educate members of Congress on developments in IoT technology and the opportunities afforded by the network connectivity of devices. In May 2017, the Congressional Caucus on Virtual, Augmented and Mixed Reality Technologies was formed “to promote the advancing technologies of virtual reality, augmented reality and mixed reality to Members of Congress and their teams.”

444

445

4.2 State Legislation Regarding Blockchain Technology and Virtual Currency

Beyond the complex legislative and regulatory landscape at the federal level, virtual currency and blockchain-related businesses also face a patchwork of various state laws. So far, New York is the only state to implement a licensing scheme specifically for anyone engaged in virtual currency-related activities. Other states may (or may not) require businesses engaged in certain transactions involving virtual currencies to be licensed under state money transmission laws. Additionally, a few states have enacted, or are considering, legislation regarding the use of virtual currencies.

440 Id. at pp. 225-226.

441 Id. at p. 226.

442 Id.

443 Id.


With state law varied and in flux, individuals and businesses in the crypto-community should be cautious and research the laws for each of the states where they intend to operate.

### 4.2.1 State Regulation Specifically for Virtual Currency Businesses

#### 4.2.1.1 New York’s BitLicense

New York was the first state to introduce a regulatory scheme directly addressing virtual currencies. In 2015, the New York Department of Financial Services (NYDFS) promulgated a set of regulations known informally as “New York’s BitLicense” or the “BitLicense.” The regulations apply to a specific list of “virtual currency business activities” involving New York or a New York resident: (1) receiving virtual currency for transmission or transmitting it, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of virtual currency; (2) storing, holding, or maintaining custody or control of virtual currency on behalf of others; (3) buying and selling virtual currency as a customer business; (4) performing exchange services as a customer business; or (5) controlling, administering, or issuing virtual currency. The development and dissemination of software in and of itself does not constitute virtual currency business activity.

The BitLicense requirements do not apply to: (1) entities that are chartered under the state’s banking law and that are approved by the Superintendent of Financial Services to engage in virtual currency business activity; or (2) merchants and consumers that use virtual currencies solely for the purchase or sale of goods and services, or for investment purposes.

Under the BitLicense regulatory scheme, an entity must file an application for a license with the NYDFS before engaging in any virtual currency business activity. The application is comprehensive and requires detailed information about participants in the business, including detailed biographical and financial information about principal officers, stockholders, and beneficiaries of the applicant as well as one or more background reports prepared by independent

---

446 23 NYCRR § 200.1, *et seq.*

447 Under New York law, ‘Virtual Currency’ “means any type of digital unit that is used as a medium of exchange or a form of digitally stored value. Virtual Currency shall be broadly construed to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort.” 23 NYCRR § 200.2(p). Those that reside, are located, have a place of business, or are conducting business in the state are considered New York residents under the regulations. 23 NYCRR § 200.2(h).

448 23 NYCRR § 200.2(d) (‘[e]xchange Service’ “means the conversion or exchange of Fiat Currency or other value into Virtual Currency, the conversion or exchange of Virtual Currency into Fiat Currency or other value, or the conversion or exchange of one form of Virtual Currency into another form of Virtual Currency”).

449 23 NYCRR § 200.2(q).

450 23 NYCRR § 200.3(c)(1).

451 23 NYCRR § 200.3(c)(2).

452 23 NYCRR § 200.3(a).
investigatory agencies. Additionally, extensive information concerning the applicant is required, including an organizational chart, current and projected financials, a description of the applicant’s business, details of all banking arrangements, written policies and procedures required under the regulations, an affidavit describing any pending or threatened actions, all litigation, and all proceedings before any governmental agency, copies of insurance policies, verification from the New York State Department of Taxation and Finance as to compliance with all state tax obligations, explanation of the methodology used to calculate the value of virtual currency to fiat currency, and a demonstration of how the applicant will comply with the BitLicense regime.

Applicants must also pay a non-refundable $5,000 fee.

As an alternative, the NYDFS may issue an applicant a conditional BitLicense, in the event that the applicant does not satisfy all of the regulatory licensing requirements. This conditional license may not exceed two years. When granting a conditional license, the Superintendent may consider the following: (i) the nature and scope of the applicant’s business; (ii) the anticipated volume of business to be transacted by the applicant; (iii) the nature and scope of the risks that the applicant’s business presents to consumers, virtual currency markets, financial markets and the general public; (iv) the measures which the applicant has taken to limit or mitigate risks that its business presents; (v) whether the applicant is registered with FinCEN; (vi) whether the applicant is licensed, registered or authorized by any governmental authority to engage in financial services or other business activities; (vii) the applicant’s financial services or other business experience; and (viii) the applicant’s history as a holder of a conditional license issued by the Superintendent. Conditional licenses may be subject to heightened review both in scope and frequency of examination or otherwise. The NYDFS must approve or deny an application within 90 days of when it deems it to be complete, subject to any extension granted by the Superintendent.

Among other things, the BitLicense requires licensees to: (1) maintain and enforce written policies, including policies and procedures for anti-fraud, anti-money laundering, cyber security, privacy and information security, and customer complaints; (2) maintain sufficient capital (either in the form of cash, virtual currency, or high-quality, highly liquid, investment-grade assets) in an amount set by the Superintendent based on various risk factors, including the licensee’s assets and liabilities, and its volume of activity; (3) maintain a surety bond or trust account to protect

453 23 NYCRR § 200.4(a).
454 23 NYCRR § 200.4(a) and (b).
455 23 NYCRR § 200.5.
456 23 NYCRR § 200.4(c).
457 23 NYCRR § 200.4(c)(3).
458 23 NYCRR § 200.4(c)(7)(i-viii).
459 23 NYCRR § 200.4(c)(2).
460 23 NYCRR § 200.6(b).
461 23 NYCRR § 200.7(c).
462 23 NYCRR § 200.8.
customers;\textsuperscript{463} (4) obtain written approval from the Superintendent for any material change to the business or offering of new products and services, or for a change of control of the business;\textsuperscript{464} (5) maintain for seven years records of virtual currency business activities, such as transaction records (e.g., names, accounts numbers, and addresses of customers), bank statements, AML records, communications and investigations related to customer complaints, and copies of advertisements;\textsuperscript{465} (6) permit the Superintendent to examine all of the licensee’s books, records, accounts, documents, or other information at a minimum every two calendar years;\textsuperscript{466} (7) submit documents and disclosures, including quarterly and annual financial statements, notifications of criminal actions or insolvency proceedings against the licensee or any of its directors and officers, and reports of any violations of BitLicense requirements;\textsuperscript{467} (8) maintain AML and cybersecurity programs, and submit reports to government authorities;\textsuperscript{468} (9) make various consumer protection disclosures to customers and provide them with receipts for their transactions;\textsuperscript{469} and (10) provide contact information on the licensee’s website, so that customers may file complaints with the company.\textsuperscript{470}

The Superintendent has the discretion to suspend or revoke a license: (1) on any ground for which the issuance of an original license may be refused; (2) for any violation of the BitLicense regulations; (3) for good cause (e.g., if the licensee defaults or is likely to default in performing its obligations, or engages in unlawful/dishonest conduct that may harm the public); or (4) for failure to pay a court judgment.\textsuperscript{471}

The BitLicense regulation is silent on penalties for noncompliance; however, the NYDFS’s regulations provide that all regulated entities are subject to all applicable penalties, including late fees and interest, provided under the state Banking Law, Financial Services Law, State Finance Law, or any other applicable law.\textsuperscript{472}

The BitLicense scheme has come under heavy scrutiny from the crypto community for stifling the new technology by invading customer privacy and imposing excessive costs and

\begin{align*}
\textsuperscript{463} & 23 \text{ NYCRR} \S 200.9. \\
\textsuperscript{464} & 23 \text{ NYCRR} \S\S 200.10, 200.11. \\
\textsuperscript{465} & 23 \text{ NYCRR} \S\S 200.12, 200.18(b). \\
\textsuperscript{466} & 23 \text{ NYCRR} \S 200.13. \\
\textsuperscript{467} & 23 \text{ NYCRR} \S 200.14. \\
\textsuperscript{468} & 23 \text{ NYCRR} \S\S 200.15, 200.16. \\
\textsuperscript{469} & 23 \text{ NYCRR} \S 200.19. \\
\textsuperscript{470} & 23 \text{ NYCRR} \S 200.20. \\
\textsuperscript{471} & 23 \text{ NYCRR} \S 200.6(c). \\
\textsuperscript{472} & 23 \text{ NYCRR} \S\S 200.6(c), 501.5. \\
\end{align*}
Many start-ups left New York, and those that remained faced an application process costing up to $100,000, including legal fees, application fee, and thousands of hours of manpower to gather and prepare the requisite documentation. These threshold costs are also a gamble for new companies given that approval is not guaranteed. Since the BitLicense regulations were issued in 2015, the NYDFS has received at least 22 applications. As of November 2018, it has issued only 12 licenses.

### 4.2.1.2 Challenges to BitLicense and the NYDFS’s Authority

There are several pending challenges to the BitLicense regulations, making the future of the BitLicense uncertain. In October 2015, Theo Chino, a bitcoin advocate and entrepreneur who was denied a BitLicense, initiated an Article 78 proceeding in New York Supreme Court, challenging BitLicense regulations. Chino alleged that the NYDFS exceeded its authority and “cross[ed] the line of administrative rule-making into the forbidden realm of legislative action” by promulgating regulations concerning virtual currency.

On May 30, 2017, Chino filed an amended complaint and an Article 78 petition asserting that the NYDFS had exceeded its jurisdiction, because the New York legislature only authorized it to regulate “financial products and services,” which he claimed bitcoin was not. Chino further alleges that the regulations are arbitrary and capricious for numerous reasons, including that the term “virtual currency,” as defined, could be construed to include all Internet activity; the regulations could include non-financial uses of blockchain technology and microtransactions; the

---


478 Article 78 proceedings are special proceedings initiated under N.Y. C.P.L.R. 7801, et seq., challenging the actions of administrative agencies on certain limited grounds. N.Y. C.P.L.R. 7803.


regulations fail to define important terms; and the regulations impose, without any rational basis, different AML obligations on virtual currency businesses than fiat currency transmitters.481 Chino also claims that the BitLicense is preempted by the Dodd-Frank Act,482 and that portions of its framework violate the First Amendment of the U.S. and New York Constitutions.483

The NYDFS filed a motion to dismiss, which was heard on October 10, 2017. The motion was granted on December 27, 2017 on the grounds that Chino lacked standing to challenge the regulation.484 Chino filed an appeal on February 4, 2018, asserting that he had suffered “injury in fact” and was “within the zone of interests or concerns sought to be promoted or protected by the statutory provision under which the agency has acted.”485 As of December 2018, the appeal is pending.486

4.2.2 State Laws for the Licensing of Money Transmitters and Money Services Businesses

In general terms, money transmission is the act of moving funds money between bank accounts or from one person or organization to another. All states except Montana487 have some form of regulations for the licensing of money transmitters, but the scope varies. Some state statutes expressly include virtual currency; New Hampshire’s expressly excludes it;488 and other state statutes are silent on the subject. Further complicating the matter, some state agencies have interpreted state law to cover virtual currency transactions, while others have found otherwise.

---

481 Id. at ¶ 103-121.
482 Id. at ¶ 122-128.
483 Id. at ¶ 129-144.
487 Division of Banking and Financial Institutions, Department of Administration, Montana, https://banking.mt.gov/moneytransmitters.
4.2.2.1 States Money Transmission Laws That Expressly Cover Virtual Currency or Have Been Interpreted to Include Virtual Currency

Several states have money transmitter laws that expressly cover virtual currency, either in the definition of “money transmission” or “monetary value.” Some states require that an individual or business engaging in virtual currency transmission obtain a license, while Alaska and Wisconsin require that the virtual currency transmitter enter into limited licensing agreements with specified state agencies.

Hawaii also requires a license to engage in the business of money transmission. The state’s regulatory agency, the Hawaii Division of Financial Institutions, has interpreted the state’s money transmission statute to apply to virtual currency exchanges. And in early 2017, the agency informed Coinbase, the only virtual currency exchange then operating in Hawaii, that it must maintain cash reserves in an amount equal to the aggregate face value of virtual currency funds.


490 The definition of ‘money transmission’ in each state’s statute is similar. Compare Ala. Code § 8-7A-2(10) (defining ‘money transmission’ as “[s]elling or issuing payment instruments, stored value, or receiving money or monetary value for transmission”) with Conn. Gen. Stat. Ann. § 36a-596(8) (defining ‘money transmission’ as “engaging in the business of issuing or selling payment instruments or stored value, receiving money or monetary value for current or future transmission or the business of transmitting money or monetary value within the United States or to locations outside the United States by any and all means including, but not limited to, payment instrument, wire, facsimile or electronic transfer”); see also Ga. Code Ann. § 7-1-680(13) N.C. Gen. Stat. Ann. § 53-208.42(13); Alaska House Bill 180 (March 14, 2017); Vt. Stat. Ann. tit. 8, § 2500(11), § 2500(22); Wash. Rev. Code Ann. § 19.230.010(18).

491 Alabama defines ‘monetary value’ as “A medium of exchange, including virtual or fiat currencies, whether or not redeemable in money.” Ala. Code § 8-7A-2(8). Connecticut defines ‘virtual currency’ as “any type of digital unit that is used as a medium of exchange or a form of digitally stored value or that is incorporated into payment system technology,” and defines ‘monetary value’ as “a medium of exchange, whether or not redeemable in money.” Conn. Gen. Stat. Ann. § 36a-596(7), (16). Georgia defines ‘virtual currency’ as a “digital representation of monetary value that does not have legal tender status as recognized by the United States government.” Ga. Code Ann. § 7-1-680(26).

held on behalf of its customers. As a result of the DFI’s interpretation, Coinbase ceased operations in Hawaii, stating that the policy “would siphon millions of dollars away from critical operations, recruitment and retention of expert staff” by requiring the company to hold the equivalent cash value of every unit of virtual currency held for a Hawaii customer as redundant collateral.

While Hawaii’s money transmission statute is similar to those of other states, none of the latter have been interpreted to impose collateral requirements like Hawaii’s. Currently, no virtual currency exchanges have applied for or obtained licenses to operate in Hawaii.

4.2.2.2 State Money Transmission Laws That Expressly Exclude Virtual Currency

The definition of “monetary value” in New Hampshire’s money transmission statute includes convertible virtual currency. However, New Hampshire House Bill 436, signed into law on June 2, 2017, and effective on August 1, 2017, amended Section 399-G:3 of the New Hampshire Revised Statutes to exempt “[p]ersons who engage in the business of selling or issuing payment instruments or stored value solely in the form of convertible virtual currency or receive convertible virtual currency for transmission to another location.” These persons do, however, remain subject to the state’s consumer protection statute.

4.2.2.3 State Money Transmission Laws That Are Silent on Virtual Currency

The money transmission laws of the remaining states and Washington, D.C., do not expressly address virtual currency. Regulators in Idaho, Illinois, Kansas, Tennessee, and Texas have nevertheless provided some guidance.

Idaho’s Department of Finance has determined that the Idaho Money Transmitters Act does not apply to any exchange that does not include the introduction or payout of fiat currency.

---


494 Id.

495 “Convertible virtual currency” means a digital representation of value that (a) can be a medium of exchange, a unit of account, and/or a store of value; (b) has an equivalent value in real currency or acts as a substitute for real currency; (c) may be centralized or decentralized; and (d) can be exchanged for currency or other convertible virtual currency. N.H. Rev. Stat. Ann. § 399-G:1.


497 Id.

Thus, a firm that only exchanges one form of virtual currency for another (e.g., bitcoin for Ether) is not currently regulated under Idaho’s money transmitter law.

Additionally, a virtual currency exchanger that sells its own inventory of virtual currency for fiat currency does not fall within the scope of the Idaho Money Transmitters Act; however, “an exchanger that holds customer funds while arranging a satisfactory buy/sell order with a third party, and transmits virtual currency and fiat currency between buyer and seller, will typically be considered a virtual currency transmitter.”499 For example, Idaho does not require a money transmitter license to operate a bitcoin ATM that sells bitcoin in exchange for a customer’s fiat currency,500 but does require a license to facilitate a bitcoin-to-fiat-currency transaction between two parties by holding the bitcoin until further instructions are given.501

Regulators in Illinois, Kansas, Tennessee, and Texas have all determined that their state’s statute does not cover virtual currencies, reasoning that virtual currencies either are not “money”


or lack “monetary value.” However, these same regulators have issued the caveat that, if virtual currency transactions also involve fiat currency, state money transmission laws may still apply.

In Florida, a state court has ruled that a virtual currency seller did not violate the state’s money transmission laws by operating without a license. Under Florida law, a person may not operate a money service business (defined to include a person acting as a payment instrument seller or a money transmitter) without a license. The statute defines a ‘money transmitter’ as a business that “receives currency, monetary value, or payment instruments for the purpose of transmitting the same by any means,” and a ‘payment instrument seller’ as a business that sells “a check, draft, warrant, money order, travelers check, electronic instrument, or other instrument, payment of money, or monetary value whether or not negotiable.”

The Florida court focused on the term “transmit,” likening a money transmitter to a middleman in a financial transaction. The court compared the activities of a money transmitter like Western Union, which takes money from person A and transmits it to person B at person A’s


503 Ill. Dep’t of Fin. and Prof’l Regulation, supra note 502 (virtual currencies are not “money” as they are not authorized or adopted by a government); Kan. Office of the State Banking Comm’r, supra note 502 (virtual currencies are not “money” as they are not authorized or adopted by a government, and they are not “monetary value” as they are not generally accepted forms of payment); Gonzales, supra note 502 (virtual currencies are not “money”); Cooper, supra note 502 (virtual currencies are not “money” or “monetary value” as they are not fiat currencies or claims of rights).


506 The court referred to the definition of “transmit” from Black’s Law Dictionary: “to send or transfer (a thing) from one person or place to another.” Order Granting Def.’s Mot. to Dismiss the Information, Florida v. Espinoza, No. F14-2923 at p. 4 (Fla. Cir. Ct. Jul. 22, 2016).
instructions, to the defendant’s activities of purchasing bitcoin at below market value and selling it to customers at a markup, reasoning that the defendant was not a money transmitter because it did not act as a middleman. Further, the court concluded that the defendant was not a payment instrument seller because virtual currency is not included in the definition of “payment instrument” and is considered property by the IRS.\textsuperscript{507}

In \textit{United States v. Murgio}, a New York federal court held that Florida’s money transmitter law applied to a bitcoin exchange.\textsuperscript{508} In contrast to \textit{Espinoza}, the \textit{Murgio} court concluded that bitcoin is a medium of exchange and thus is a form of “monetary value”\textsuperscript{509} under Florida’s definitions of “money transmitter” and “payment instrument.”\textsuperscript{510} The \textit{Murgio} court criticized the \textit{Espinoza} court’s analysis on the grounds that it failed to analyze whether virtual currency qualifies as “monetary value” and relied on the IRS’s classification without explaining its relevance.\textsuperscript{511}

Thus, whether a virtual currency business is required to obtain a state money transmission license often depends on the particular activity at issue and the language of a particular state’s statute. If a state’s money transmission law includes the terms “monetary value” or “stored value,” and the terms are broadly defined, as in Vermont and Hawaii, then a virtual currency business may be required to obtain a money transmitter license. However, if a state’s statute only includes the term “money” (which is generally defined as a medium of exchange authorized or adopted by a domestic or foreign government) or a narrow definition of “monetary value” or “stored value,” like in Illinois, Kansas, Tennessee, and Texas, then a virtual currency business may not need a money transmitter license unless that business intends to conduct transactions involving fiat currency.

\textbf{4.2.2.4 Specific Requirements of State Money Transmission Laws}

Although application procedures differ, each state generally requires payment of an application fee and submission of detailed information and documents, including: personal information of the applicant and its officers and directors; information on criminal convictions and bankruptcy; information on services to be provided, business plan, and business structure; financial documents; and banking information.

Licensees must also have a surety bond, generally in an amount determined by the regulating agency, to protect consumers. Required bond amounts range from $10,000 (Washington)\textsuperscript{512} to $5 million (Alabama).\textsuperscript{513} Connecticut specifically gives the state banking commissioner discretion to set the bond amount based on the current and prospective volatility of

\begin{itemize}
  \item \textsuperscript{507} \textit{Id.} at p. 5.
  \item \textsuperscript{508} \textit{United States v. Murgio}, 209 F. Supp. 3d 698 (S.D.N.Y. 2016).
  \item \textsuperscript{509} Florida statute defines “monetary value” as “a medium of exchange, whether or not redeemable in currency.” Fla. Stat. Ann. § 560.103(21).
  \item \textsuperscript{510} \textit{Murgio}, 209 F. Supp. 3d at 712-14.
  \item \textsuperscript{511} \textit{Id.} at 713.
  \item \textsuperscript{512} Wash. Rev. Code Ann. § 19.230.050(1).
  \item \textsuperscript{513} Ala. Code § 8-7A-7(g).
\end{itemize}
the virtual currency market for licensees that transmit monetary value in the form of virtual currency at issue.\textsuperscript{514}

Each state also requires licensees to maintain a certain level of net worth based on generally accepted accounting principles. For example, Alabama requires a licensee to maintain a net worth of $25,000,\textsuperscript{515} while Washington gives its Director of Financial Institutions the discretion to set the requirement anywhere between $10,000 and $3 million.\textsuperscript{516}

Each state also imposes recordkeeping\textsuperscript{517} and reporting requirements\textsuperscript{518} (e.g., annual reports, and reports or notices of material changes in information). Some states also expressly require licensees to comply with federal AML laws.\textsuperscript{519}

Violations of the licensing statutes can result in suspension or revocation.\textsuperscript{520} Regulatory agencies can also impose civil penalties, order restitution, and obtain court-ordered injunctions.\textsuperscript{521} Violations can even result in criminal liability. In Washington, for example, depending on the violation, an alleged violator may face misdemeanor, gross misdemeanor, or even Class C felony charges.\textsuperscript{522}

4.2.3 Other State Blockchain and Cryptocurrency Legislation

Enacted on March 29, 2017, Arizona House Bill 2417 gives legal effect to signatures and records secured on a blockchain. The law provides that “a contract relating to a transaction may not be denied legal effect, validity or enforceability solely because that contract contains [an electronic distributed code contract] term.”\textsuperscript{523} The law also states that people who use blockchain technology to secure information retain rights of ownership with respect to their information, subject to their agreement to transfer those rights.\textsuperscript{524} On August 9, 2017, Arizona Statute § 13-3122 was enacted, making it unlawful to require people to use or be subject to electronic firearm-tracking technology (including distributed ledger or blockchain technology).\textsuperscript{525} In April 2018, Arizona enacted House Bill 2602, which prohibits cities, towns, and counties from regulating the

\begin{footnotesize}
\begin{enumerate}
\item Ala. Code § 8-7A-10.
\item Ariz. Rev. Stat. § 44-7061.
\item Id.
\end{enumerate}
\end{footnotesize}
running of blockchain nodes in a residence in order to foster the development of blockchain technology,526 and House Bill 2603, which allows corporations to hold and share data on a distributed ledger.527

Enacted on April 26, 2017, West Virginia House Bill 2585, codified as W. Va. Code Ann. § 61-15-1, et seq., amended the state’s penal code to create an offense for money laundering. The law now makes it “unlawful for any person to conduct or attempt to conduct a financial transaction involving the proceeds of criminal activity knowing that the property involved in the financial transaction represents the proceeds of, or is derived directly or indirectly from the proceeds of, criminal activity.”528 The definition of “financial transaction” now includes the use of a “monetary instrument,”529 which in turn is defined to include cryptocurrency530 (i.e., “digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, and which operate independently of a central bank”).531 The law further provides that property involved in the violation could be subject to forfeiture, and allows a court to direct the disgorgement to a victim of any property or monetary instrument involved in the violation.

Enacted on June 5, 2017, Nevada Senate Bill 398 amended the Nevada Uniform Electronic Transactions Act by inserting the term ‘blockchain’ in the definition of ‘electronic record,’ thereby giving legal effect to electronic distributed code contracts and other blockchain-based records.532 The bill further inserted provisions in the Nevada Revised Statutes prohibiting local governments from: “(1) imposing a tax or fee on the use of a blockchain; (2) requiring a certificate, license or permit to use a blockchain; and (3) imposing any other requirement relating to the use of a blockchain.”533

Enacted on July 21, 2017, Delaware Senate Bill 69 amended the state’s General Corporation Law to provide statutory authority for state corporations to use blockchain technology for the creation and maintenance of corporate records, including the corporation stock ledger, in which all issuances and transfers of a corporation’s shares are recorded.534 On July 23, 2018, Delaware enacted three additional bills amending the Delaware Revised Uniform Limited Partnership Act,535 the Delaware Limited Liability Company Act,536 and the Delaware Statutory

---

534 8 Del. C. § 224.
535 6 Del. C. § 17-104(g), 6 Del. C. § 17-302(e), 6 Del. C. § 17-305(c), and 6 Del. C. § 17-405(d).
536 6 Del. C. § 18-104(g), 6 Del. C. § 18-302(d), 6 Del. C. § 18-305(d), and 6 De. C. § 18-404(d).
Trust Act, permitting the use of distributed ledger technology to carry out certain corporate governance functions.

Enacted on October 6, 2017, Alaska’s Revised Uniform Fiduciary Access to Digital Assets Act establishes the manner in which an individual’s digital assets, including cryptocurrency, can be handled by a trusted custodian. The Act makes specific mention of cryptocurrencies, and any Alaskan is now allowed to use online tools to direct a custodian to transfer cryptocurrency to a designated recipient. As an alternative, individuals can still use a will, trust, or other record to achieve the same purpose. The Act is only applicable to a custodian if the user resides in Alaska or resided there at the time of the user’s death. The law went into effect on October 31, 2017. Maine enacted an identical Revised Uniform Fiduciary Access to Digital Assets Act on April 4, 2018.

Enacted on March 22, 2018, Tennessee Senate Bill 1662, which amended Tennessee Code Annotated, Title 47, Chapter 10, treats blockchain-based signatures as binding electronic signatures. Additionally, the law explicitly recognizes the legitimacy of “smart contracts” by stating: “No contract relating to a transaction shall be denied legal effect, validity, or enforceability solely because that contract contains a smart contract term.” It also contains a provision that, “protects ownership rights of certain information secured by blockchain technology.”

In March of 2018, the Wyoming legislature passed four bills related to blockchain technology and cryptocurrency, which Governor Matt Mead signed in April 2018:

- House Bill 19, The Wyoming Money Transmitter Act, exempts virtual currencies from Wyoming’s money transmitter laws, which permitted virtual

---

537 12 Del. C. § 3801(a), 12 Del. C. § 3806(f)(2), 12 Del. C. § 3806(g)(2), and 12 Del. C. § 3819(d).
538 Alaska Stat. § 13.63.010 et seq.
539 Id.
540 Id.
541 Id.
543 Tenn. Code Ann. § 47-10-201 et seq.
544 The law defines a “smart contract” as “an event-driven computer program, that executes on an electronic, distributed, decentralized, shared, and replicated ledger that is used to automate transactions, including, but not limited to, transactions that: (a) take custody over and instruct transfer of assets on that ledger; (b) create and distribute electronic assets; (c) synchronize information; or (d) manage identity and user access to software applications.”
546 Id.
547 HB19 defines virtual currency as “any type of digital representation of value that: (a) is used as a medium of exchange, unit or account or store of value; and (b) is not recognized as legal tender by the United States government.”
currency exchanges to resume operations within the state. Companies such as Coinbase had ceased operations in Wyoming in 2016.\footnote{Gary Miller, \textit{Blockchain Valley: Wyoming is Poised to Become the Cryptocurrency Capital of America}, Newsweek (Mar. 2, 2018), \url{http://www.newsweek.com/wyoming-cowboy-state-poised-today-become-blockchain-valley-828124}.}

- House Bill 70, Open Blockchain Tokens-Exemptions, also known as the Utility Token Bill, exempts certain digital assets such as utility tokens from Wyoming’s securities laws. Utility tokens are made available by a person or group who provides or creates the platform to offer some good or service.\footnote{Id.}

- House Bill 101, the Electronic Corporate Records, also known as The Blockchain Records Bill, amends Wyoming’s Business Corporations Act to permit blockchain-based records storage, shareholder management, and shareholder votes. This bill is similar to the modifications that Delaware made to its corporate code in July 2017.\footnote{Id.}

- House Bill 126, the Limited Liability Companies-Series, allows limited liability companies to “establish series of members, managers, transferable interests or assets as specified; specifying powers; providing for limitations on liabilities; providing for management, termination and dissolution; authorizing distributions to members; imposing a requirement on foreign limited liability companies that establish series; requiring rulemaking; and providing for effective dates.”

In May 2018, Vermont’s Governor, Phil Scott, signed into law an act that creates a new type of entity called a “blockchain-based limited liability company” (“BBLLC”). In order to obtain this status, an entity must elect it in its articles of organization and the entity’s operating agreement must, in a summary description of the mission or purpose of the BBLLC, “specify whether the decentralized consensus ledger or database utilized or enabled by the BBLLC will be fully decentralized or partially public or private, including the extent of participants’ access to information and read and write permissions with respect to protocols,” adopt voting procedures, which may include smart contracts to address a variety of intercompany issues, and adopt protocols for responding to securities breaches.\footnote{11 V.S.A. § 4172.}

In September 2018, California passed its first substantive blockchain law. Set to take effect on January 1, 2019, the law allows privately held corporations and social purpose organizations to keep certain legally required corporate records and communications on a blockchain, such as lists of shareholders and stock records.\footnote{Cal. Corp. Code § 204; Cal. Corp. Code § 2603.} The law does not apply to corporations that have outstanding securities listed on the New York Stock Exchange (NYSE), the NYSE Amex, the NASDAQ Global Market, or the NASDAQ Capital Market.\footnote{Cal. Corp. Code § 204(a)(12); Cal. Corp. Code § 2603(a)(12).} Additionally, the law includes a sunset

\footnotesize


549 \textit{Id.}

550 \textit{Id.}

551 11 V.S.A. § 4172.


provision, meaning that unless further legislative action is taken, it will automatically expire on January 1, 2022.554

**4.2.4 State Tax Treatment of Virtual Currency Transactions**

**4.2.4.1 Sales and Use Taxes**

Generally, sales tax is levied on retail sales of tangible personal property, and in some states, on certain services and digital goods as well. Use tax is levied on tangible personal property purchased out of state but consumed within the state. Sales and use taxes are typically calculated as a percentage of the price of the goods or services being sold or consumed. Many states combine them into single “sales and use” tax.

With the recent advent of virtual currencies, taxation authorities in some states have issued guidance concerning the use of virtual currencies as a form of payment for goods and services. These authorities have clarified that, when a retailer accepts virtual currency in exchange for goods and services, sales and use tax applies. States, however, differ on how to measure the tax. In California and Washington, the measure of tax is the amount allowed by the retailer in exchange for the virtual currency.555 As the Washington Department of Revenue has noted, the “measure of the tax is not affected by virtual currency fluctuation.”556 Both the California Board of Equalization and Washington Department of Revenue advise retailers to retain documentation (e.g., a copy of the menu) when payment is made of the amount that the retailer regularly charges in sales of the same or similar property.557

Several states take a different approach from California and Washington, basing sales and use tax on the amount of virtual currency received. In Kentucky, the tax is based on the amount of virtual currency accepted by the business. The Kentucky Department of Revenue requires businesses to convert the virtual currency that is accepted as a form of payment into U.S. dollars.

---

554 Cal. Corp. Code § 204(e); Cal. Corp. Code § 2603(e).


556 Wash. St. Dep’t of Revenue, *supra* note 556.

before applying a “6 percent Kentucky sales and use tax” to the transaction.\textsuperscript{558} The Kentucky Department of Revenue further instructs businesses to maintain documentation of the value of the virtual currency at the time of the transaction.\textsuperscript{559}

Like Kentucky, New Jersey’s Division of Taxation has issued a Tax Advisory Memorandum advising retailers of taxable goods and services who accept virtual currency to “determine the fair market value of the currency in U.S. dollars as of the date of payment and charge the purchaser sales tax on the underlying transaction.”\textsuperscript{560} New York also requires sales tax to be “based on the market value of the convertible virtual currency at the time of the transaction, converted to U.S. dollars.”\textsuperscript{561} Also, Wisconsin’s Department of Revenue states that sales tax “is computed on the value of the consideration received by the seller, measured in U.S. dollars as of the date that the virtual currency is received.”\textsuperscript{562}

Minnesota’s Department of Revenue states that virtual currency “should be treated as cash,” but has not clarified whether sales and use tax should apply based on the amount allowed by the retailer (as with California) or based on the amount of virtual currency accepted (as with Kentucky).\textsuperscript{563}

With respect to the purchase or sale of virtual currency, Missouri’s Department of Revenue advises that sales and use tax does not apply, since virtual currency is an intangible property.\textsuperscript{564} Similar determinations have been made by New Jersey’s Division of Taxation, New York’s Department of Taxation and Finance, and Wisconsin’s Department of Revenue.\textsuperscript{565}


\textsuperscript{559} Id.


\textsuperscript{561} N.Y. State Dep’t of Tax’n and Fin., Taxpayer Guidance Div., Technical Memorandum, \textit{Tax Department Policy on Transactions Using Convertible Virtual Currency} (Dec. 5, 2014), \url{https://www.tax.ny.gov/pdf/memos/multitax/m14_5c_7i_17s.pdf?_ga=1.154726968.1491961374.1457722926}.

\textsuperscript{562} Wis. Dep’t of Revenue, \textit{Sales and Use Tax Report} (Mar. 2014), \url{https://www.revenue.wi.gov/SalesUseTaxReport/14-1.pdf}.

\textsuperscript{563} Minn. Dep’t of Revenue, Sales Tax Fact Sheet 167, \textit{Coupons, Discounts, Rewards, Rebates, and Other Forms of Payment} (Jun. 2015), \url{http://www.revenue.state.mn.us/businesses/sut/factsheets/FS167.pdf}, (last updated Sept. 2018).

\textsuperscript{564} Mo. Dep’t of Revenue, LR7411, \textit{Collection of Sales Tax on Bitcoin Transfers Through an Automated Teller Machine (ATM)} (Sep. 12, 2014).

\textsuperscript{565} N.J. Div. of Tax’n, \textit{supra} note 560; N.Y. State Dep’t of Tax’n and Fin., \textit{supra} note 561; Wis. Dep’t of Revenue, \textit{supra} note 562.
4.2.4.2 Other State Taxes

In light of the IRS’s decision to treat virtual currency as property, the New Jersey Division of Taxation advises:

In general, the Corporation Business Tax Act follows the federal determination of taxable income. The Gross Income Tax Act follows the federal treatment of the gain or loss from the sale or exchange of property. In addition, the fair market value of convertible virtual currency paid as wages is subject to New Jersey gross income tax withholding. An independent contractor that receives convertible virtual currency for services performed must determine the fair market value of the currency in U.S. dollars as of the date received. A payment made using convertible virtual currency is subject to information reporting requirements to the same extent as any other payment made in property.566

New York law similarly provides:

For corporation tax and personal income tax purposes, New York State Tax Law conforms to the federal treatment of convertible virtual currency as detailed in IRS Notice-2014-21. The notice provides that convertible virtual currency is treated as property for U.S. federal tax purposes. General tax principles that apply to property transactions apply to transactions using convertible virtual currency.567

4.2.4.3 Bills to Study Blockchain Technology

Enacted on June 8, 2017, Vermont Senate Bill 135, among other things, instructed the Center for Legal Innovation at Vermont Law School, in consultation with various government officials, to submit a report to the General Assembly by November 30, 2017, that includes:

(a) findings and recommendations on the potential opportunities and risks presented by developments in financial technology [including blockchain technology]; (b) suggestions for an overall policy direction and proposals for legislative and regulatory action that would effectively implement that policy direction; and (c) measurable goals and outcomes that would indicate success in the implementation of such a policy.

On December 7, 2017, the Center for Legal Innovation at Vermont Law School submitted the Financial Technology Report summarizing that the Vermont legislature “act carefully but still boldly in developing a legislative response to the opportunities and concerns raised by FinTech generally and blockchain in particular.”568

Adopted by both houses of the Illinois legislature on June 28, 2017, Illinois House Joint Resolution 25 created the Illinois Legislative Blockchain and Distributed Ledger Task Force to study the feasibility of using blockchain technology for recordkeeping and service delivery by

566 N.J. Div. of Tax’n, supra note 560.
567 N.Y. State Dep’t of Tax’n and Fin., supra note 561.
state and local governments. The Task Force is instructed to research, analyze, and consider the risks associated with blockchain technology, different types of blockchains, current use cases under development, and the modification of state law to facilitate paperless recordkeeping. On January 31, 2018, the Task Force released a report, which stated in part, “this Task Force believes that blockchain technology and its built-in encryption can facilitate highly-secure methods for interacting with government and keeping paperless records, increasing data accuracy and providing better cybersecurity protections for Illinois residents.”

In early 2018, both New York (AB09862) and New Jersey (AB3613) put forth bills to study blockchain technology. The New York taskforce will be assessing the impact of “economic empowerment zones” for cryptocurrency mining, whereas while the New Jersey task force will study “whether state, county and municipal governments can benefit from a transition to a Blockchain-based system for recordkeeping and service delivery.” Both bills have been referred to a committee.

In June 2018, Connecticut governor Dannel Malloy signed into law SB443, which establishes a working group to study blockchain technology and create a master plan for “fostering the expansion of the blockchain industry in the state.” The working group will: “(1) identify the economic growth and development opportunities presented by blockchain technology; (2) assess the existing blockchain industry in the state; (3) review workforce needs and academic programs required to build blockchain expertise across all relevant industries; and (4) make legislative recommendations that will help promote innovation and economic growth by reducing barriers to and expediting the expansion of the state’s blockchain industry.”

4.2.5 Uniform Law Commission

The Uniform Law Commission (ULC), also known as the National Conference of Commissioners on Uniform State Laws, voted to finalize and approve the proposed uniform regulations for virtual currency, titled the Uniform Regulation of Virtual Currency Businesses Act (VCBA). Despite opposition from many in the crypto community, on July 19, 2017, members of

---


571 New Jersey Assembly Bill No. 3613, (Mar. 12, 2018), http://www.njleg.state.nj.us/2018/Bills/A4000/3613_I1.HTM.


573 The ULC is a non-profit unincorporated association, comprised of state commissions on uniform laws from each state, the District of Columbia, the Commonwealth of Puerto Rico, and the U.S. Virgin Islands. The ULC’s sole purpose is to study and review the law of the states to determine which areas of law should be uniform.

The VCBA requires a license for any person to engage in “virtual currency business activity,” defined as:

1) Exchanging, transferring, or storing virtual currency\footnote{‘Virtual Currency’ is defined under the VCBA as “(A) a digital representation of value that: (1) is used as a medium of exchange, unit of account, or store of value; and (2) is not legal tender, whether or not denominated in legal tender; and (B) does not include: (1) a transaction in which a merchant grants value as part of an affinity or rewards program, which value cannot be taken from or exchanged with the merchant for legal tender, bank credit, or virtual currency; or (2) a digital representation of value issued by or on behalf of the publisher and used within an online game, game platform, or family of games sold by the same publisher or offered on the same game platform.” \textit{Id.}} or engaging in virtual currency administration, whether directly or through an agreement with a virtual currency control services vendor;

2) Holding electronic precious metals or electronic certificates representing interests in precious metals on behalf of another person or issuing shares or electronic certificates representing interests in precious metals; or

3) Exchanging one or more digital representations of value used within one or more online games, game platforms, or family of games for (i) virtual currency offered by or on behalf of the same publisher from which the original digital representation of value was received; or (ii) legal tender or bank credit outside the online game, game platform, or family of games offered by or on behalf of the same publisher from which the original digital representations of value was received.

The VCBA expressly does not apply to a number of entities and activities, including “(1) the exchange, transfer, storage, or administration of virtual currency, insofar as those activities are governed by federal law; (2) federal, state, and local government, and any agency or instrumentality thereof; (3) banks; (4) licensed or authorized money transmitters; (5) a person engaged in the business of dealing in foreign exchange to the extent that those activities are not governed by federal law; (6) persons that only provide connectivity software, computing power, or data storage or security services; (7) persons that use virtual currency for personal, family, household, or academic purposes (e.g., investing, buying, or selling); (7) a person whose virtual currency business activity is reasonable valued annually at $5,000 or less; (8) attorneys or title

\footnote{\textit{Id.}}
insurance companies providing escrow services; (9) securities intermediaries; (10) secured creditors or any creditor with a judicial lien or lien arising by operation of law on the virtual currency; (11) virtual-currency control-services vendor; and (12) a person that does not receive compensation from a resident for providing virtual-currency products or services, conducting virtual-currency business activities, or is engaged in testing products or services with the person's own funds.”

Similar to an application for a money transmission license, the VCBA’s application procedure requires detailed information and documentation, including (1) the name (e.g., any fictitious or trade name the applicant intends to use) and address of the applicant, its executive officers, and the person who will manage its computer servers; (2) a current and historical background of the business; (3) the name, address and telephone number of a person that manages each server that the applicant expects to use; (4) a list of the applicant’s money transmitter licenses, expiration dates, and any disciplinary actions; (5) any criminal convictions against the applicant or its officers; (6) any litigation or proceeding involving the applicant or its officers; (7) bankruptcy information; (8) banking information; (9) the source of funds and credit to be used by the applicant to conduct business; (10) insurance policies; (11) incorporation information; and (12) FinCEN registration.578

Licensees under VCBA would be required to do several things, including (1) file annual renewals containing annual financial documents and provide interim reports concerning material changes to the business; (2) maintain a certain level of net worth; (3) maintain records for five years; (4) make certain disclosures to customers; (5) maintain an amount of virtual currency sufficient to satisfy the aggregate claims of any persons whose virtual currency the licensee controls on their behalf; and (6) maintain various policies and programs, including security, business continuity, anti-money laundering, and counterterrorism financing.579

The VCBA also permits regulatory agencies to take various enforcement measures (e.g., suspension or revocation of license, issuance of a cease-and-desist order, request for a court-appointed receiver, assessment of civil penalties, or recovery of the security deposited with the agency by the licensee) if any licensee violates the act or engages in unsafe, unsound, unfair, fraudulent, or dishonest acts or practices.

578 The VCBA would further require applicants to deposit with the regulatory agency funds, a letter of credit, a surety bond, or other security in an amount set by the agency based on the nature and risk of the business. Id.

579 The VCBA also provides registration procedures for persons who engage in virtual currency business activity that does not exceed $5,000 annually. Id.
Chapter 5

5 International Regulation of Virtual Currency and Blockchain

On an international level, persons and businesses engaged in the virtual currency and blockchain technology ecosystem face myriad laws and regulations as treatment varies across borders. Currently, only a handful of countries have passed blockchain-specific regulations, while several others have attempted to adapt existing laws, such as anti-money laundering (AML) regulations, to the technology. However, similar to the United States, international governments generally view virtual currencies with heightened scrutiny, and many nations are pursuing tighter, more explicit regulations.580

5.1 Virtual Currencies as Legal Tender or a Legal Method of Payment

Legal tender, such as government-backed currency, is any official medium of payment recognized by law that can be used to extinguish a public or private debt or meet a financial obligation.581

On February 26, 2018, the Marshall Islands passed the Declaration and Issuance of the Sovereign Currency Act 2018.582 This bill states “[t]he purpose of this Act is to declare and issue a digital decentralized currency based on blockchain technology as the legal tender of the Republic of Marshall Islands.”583 The bill names the digital decentralized currency “Sovereign” or “SOV”, which it defines as “digital decentralized currency based on blockchain technology, which will be issued by the Ministry of Finance, in accordance with this Act and shall be legal tender of the Republic of Marshall Islands.”584 Neema, an Israeli start-up dedicated to facilitating international money transfers, is using a public protocol called Yokwe to develop the technology underlying the SOV.585 The Yokwe protocol is designed to minimize know-your-customer (KYC) and financial crime concerns by linking accounts to real, government-verified identities.586


583 Id. at § 302.

584 Id. at § 303(a).


586 Id.
Yokwe protocol will require users to identify themselves on the blockchain in order to be more comparable with the framework of the regulated banking industry.\footnote{Gertrude Chavez-Dreyfuss, \textit{Marshall Islands to Issue Own Sovereign Cryptocurrency}, Reuters, (Feb. 28, 2018), \url{https://www.reuters.com/article/us-crypto-currencies-marshall-islands/marshall-islands-to-issue-own-sovereign-cryptocurrency-idUSKCN1GC2UD}.}

In early 2018, the Venezuelan government announced that it would have a new national token called the Petro.\footnote{Venezuelan Financial Proposal (Jan. 30, 2018), \url{https://whitepaperdatabase.com/venezuela-petro-cryptocurrency-ptr-english-whitepaper/} (last visited Nov. 16, 2018).} According to the Petro’s whitepaper, the “Petro will be a sovereign crypto asset backed and issued by the Venezuelan State as a spearhead for the development of an independent, transparent and open digital economy open to direct participation of citizens.”\footnote{\textit{Id.} pg. 3.} Venezuelan oil assets are used to promote the adoption of the currency.\footnote{\textit{Id.}} On March 19, 2018, President Trump signed an executive order imposing new sanctions against Venezuela, alleging that Venezuela is attempting to bypass existing economic restrictions with the Petro.\footnote{\textit{Executive Order on Taking Additional Steps to Address the Situation in Venezuela}, (Mar. 19, 2018) \url{https://www.whitehouse.gov/presidential-actions/executive-order-taking-additional-steps-address-situation-venezuela/}.} The executive order also barred American citizens and residents from participating in transactions or investing in digital currencies or tokens tied to the Petro or Venezuelan government.\footnote{\textit{Id.}}


1) Property value that can be used by unspecified persons for payment of equivalent value for purchased goods, rental fees, or services, that can be purchased by or sold to unspecified persons, and that is transferable via an electronic data processing system (limited to property values that are stored electronically on electronics, excluding currency and currency denominated assets); or
2) Property value that can be mutually exchangeable for 1 above with unspecified persons and is transferable via an electronic data processing system. 595

After the amendment, many outlets reported that the status of bitcoin and other cryptocurrencies in Japan was that of a “legal tender”; however, Japan’s Financial Services Agency confirmed in 2017 that the bitcoin and other cryptocurrencies are a legally accepted means of payment, not a “legal tender” of the country. 596 On April 1, 2017, Japan officially began recognizing bitcoin and several cryptocurrencies as legal methods of payment. 597

595 Umeda, supra note 593.
596 Reuters Staff, ADVISROY-References to Bitcoin as ‘Legal Tender’ in Japan, Reuters (Dec. 13, 2017), https://uk.reuters.com/article/idUKL3N1OD35L.
5.2 Countries Where Virtual Currency is Banned

Multiple countries, including Algeria, Bolivia, Morocco, Nepal, Pakistan, and Bangladesh have proactively banned the use of virtual currencies for all purposes based on the

598 The 2018 Financial Law of Algeria prohibits the use of cryptocurrencies. It stipulates: “The purchase, sale, use, and possession of so-called virtual currency are prohibited. A virtual currency is one used by Internet users over the Internet. It is characterized by the absence of physical support such as coins, paper money, or payments by check or credit card.” Any violation of this provision is punishable in accordance with the laws and regulations in force.” Global Legal Research Directorate Staff, Libr. of Congress https://www.loc.gov/law/help/cryptocurrency/world-survey.php#algeria (last updated July 31, 2018).

599 On May 6, 2014, the Central Bank of Bolivia, El Banco Central de Bolivia, issued a resolution prohibiting the use of any currency not issued or regulated by the government. One reason the bank offered the resolution was that use of a virtual currency could cause loss to its holders because such currencies are unregulated. The Bolivian Central Bank also provided a non-exhaustive list of virtual currencies, including bitcoin. El Banco Central de Bolivia, Directory Resolution No. 044/2014 (May 6, 2014), https://www.bcb.gob.bo/webdocs/01_resoluciones/044%202014.PDF.


601 During the week of October 7, 2017, seven individuals were arrested for allegedly running illegal bitcoin exchange operations in Nepal. Nepal’s Central Investigation Bureau (CIB) explained that the individuals had violated the order of the National Bank of Nepal, which stated that until regulations are conceived, bitcoin and other cryptocurrency exchanges are illegal. Jamie Redman, Bitcoin Illegal in Nepal? Police Arrest Seven Individuals for Trading Operations, Bitcoin.com (Oct. 7, 2017), https://news.bitcoin.com/bitcoin-illegal-in-nepal-police-arrest-seven-individuals-for-trading-operations/.

602 On April 6, 2018, the SBP issued a press release cautioning the general public on the risk of virtual currencies: “[The] General Public is advised that Virtual Currencies/Coins/Tokens (like Bitcoin, Litecoin, Pakcoin, OneCoin, DasCoin, Pay Diamond etc.) are neither recognized as a Legal Tender, nor has SBP authorized or licensed any individual or entity for the issuance, sale, purchase, exchange or investment in any such Virtual Currencies/Coins/Tokens in Pakistan. Further, Banks/DFIs/Microfinance Banks and Payment System Operators (PSOs)/Payment Service Providers (PSPs) have been advised not to facilitate their customers/account holders to transact in Virtual Currencies/Initial Coin Offerings (ICOs)/Tokens. BPRD’s Circular No. 03 of 2018.” External Relations Department, (Apr. 6, 2018), http://www.sbp.org.pk/press/2018/Pr-VC-06-Apr-18.pdf.

603 On December 24, 2017, the Central Bank of Bangladesh issued a cautionary notice that cryptocurrencies are illegal in Bangladesh. According to a news report, the notice states that “[t]ransaction [sic] with this currency may cause a violation of the existing money laundering
supposed need to safeguard their citizens against fraud and financial loss, and to protect the national currency.

5.3 Chinese Government Actions Concerning Virtual Currency

It is often difficult to determine whether reports of supposed actions by the Chinese government regarding virtual currency are accurate, since the government does not always issue explanatory statements. Thus, caution should be exercised when relying on third-party accounts of actions by the Chinese government.

China has restricted financial institutions from engaging in transactions involving virtual currencies. On December 3, 2013, China’s central bank, the People’s Bank of China (PBoC), in conjunction with five ministries, issued Bank Notice No. 289, forbidding financial institutions from handling bitcoin transactions. The central bank stated that financial institutions and payment companies could not provide pricing in bitcoin, buy and sell bitcoin, or insure bitcoin-related products. Individuals and businesses that do not provide payment services were still permitted to use virtual currencies.

On September 4, 2017, the PBoC issued a statement that initial coin offerings, referred to as “token fundraising,” were “illegal and disruptive to economic and financial stability.” Under ICO Rules, ICOs that raise cryptocurrencies such as bitcoin and Ether through the irregular sale and circulation of tokens are essentially engaging in public financing without official authorization. As a result of the statement, all token fundraising in China has been halted, and all organizations that have completed a token fundraising are required to provide refunds. The statement further bars all financial and non-banking payment institutions from providing account and terrorist financing regulations.” The notice further states that bitcoin transactions “are not authorized by the Bangladesh Bank or any regulatory agencies, and do not conform with the provisions under the Foreign Exchange Regulation Act, 1947; Anti-Terrorism Act, 2009; and the Money Laundering Prevention Act, 2012.”

---


605 BTCChina, supra note 604.

606 Id.


608 Id.

609 Id.
opening, registration, trading, clearing, and settlement services for token fundraising activities. Government authorities may shut down websites and mobile applications of platforms that fail to comply, remove the applications from application stores, or even suspend the platform’s business licenses.

In mid-September 2017, the Beijing Municipal Bureau of Financial Work and the Shanghai Municipal Financial Service Office ordered virtual currency exchanges operating in Beijing and Shanghai to stop domestic trading and registration of new users. A affected exchanges are required to submit plans for the withdrawal of investor funds to protect investors. In the wake of these government orders, several virtual currency exchanges operating in Beijing and Shanghai – including BTCCChina, OkCoin, and Huobi, three of the world’s largest bitcoin exchanges – announced plans to cease domestic operations.

In mid-January of 2018, the PBoC prohibited payment providers from facilitating cryptocurrency trades. Then on February 4, 2018, it was reported that “to prevent financial risks, China would step up measures to remove any onshore or offshore platforms related to virtual currency trading or ICOs.”

Although China continues its crusade against cryptocurrency, the government seems open to using blockchain technology for purposes other than cryptocurrency. For example, on March 26, 2018, the China Banknote Blockchain Technology Research Institute, announced the rollout of the Blockchain Registry Open Platform (BROP), a new blockchain-as-a-service platform that will allow users to prove their identities and search, share, and authenticate information and

---

610 Id.
611 Id.
613 Id.
616 Id.
records on the blockchain. Other departments of the Chinese government have also reportedly been conducting special studies on blockchain technology.

5.4 Taxation of Virtual Currencies in Other Countries

Nations take different approaches to the tax treatment of virtual currencies. Some have determined that virtual currencies should be treated as a currency for income tax purposes, while others treat it as an asset.

Canada: In May 2013, the Canada Revenue Agency released an official fact sheet on its virtual currency tax rules. Where virtual currency is used to pay for goods or services, the rules for barter transactions apply – “a barter transaction occurs when any two persons agree to exchange goods or services and carry out that exchange without using legal currency.” The value of the goods purchased via virtual currency must be included in the seller’s income for tax purposes, and the amount to be included is the value of the goods in Canadian dollars.

European Union: On October 22, 2015, in a milestone decision, the European Court of Justice (ECJ) exempted bitcoin exchange transactions from Value Added Tax (VAT). The underlying dispute concerned the issue of whether VAT applied to transactions involving the conversion of virtual currency to traditional currency, and vice versa. Swedish tax authorities argued that bitcoin was a commodity, and that virtual currency exchange transactions should thus be subject to VAT. The ECJ, however, concluded otherwise. While the court acknowledged that exchange transactions using virtual currencies as a means of payment constituted a supply of

---


623 VAT is a general, broadly based consumption tax assessed on the value added to goods and services. VAT directives are made at the EU level, with each member state then transposing the measures into national law. For more information on EU VAT, see Taxation and Customs Union, What is VAT? (last visited Nov. 14, 2018), https://ec.europa.eu/taxation_customs/business/vat/what-is-vat_en.

624 Skatteverket, supra 622.

625 Id.
service for consideration, the court ultimately ruled that such exchange transactions fell within VAT exemptions relating to “currency, [and] bank notes and coins used as legal tender.”626

Recently, several countries in the EU have issued additional guidance on their tax regimes in conjunction with VAT. For example, on February 27, 2018, Germany’s Federal Ministry of Finance released a document indicating that bitcoin will not be subject to VAT, when exchanged with fiat currency, and that VAT will only be applicable when goods and services are paid for in cryptocurrency.627 Other countries such as Denmark have declared that losses on sales of bitcoins purchased as an investment are tax-deductible and that profits are subject to income taxation.628

**Israel**: In January 2018, the Israel Tax Authority issued a draft circular clarifying the income tax consequences of virtual currency activities.629 According to the circular, virtual currencies are not “currency” or “foreign currency” under the Bank of Israel Law.630 However, the Israel Tax Authority has proposed that the use of virtual currencies should be considered as a “means of virtual payment” and subject to taxation.631 Specifically, for the purpose of income tax and VAT requirements, virtual currency is viewed as “an asset” and is taxed in accordance with relevant transaction classifications.632

**Japan**: Effective on July 1, 2017, an amendment to the country’s Consumption Tax Act exempted virtual-currency-to-cash exchange transactions from the consumption tax, which is imposed on transfers of assets or provisions of services in Japan for business purposes.633

---

626 *Id.*


629 Press Release, Israel Tax Authority, *The Tax Authority Published a Draft Circular That Clarifies the Taxation of Activity in Virtual Currencies – For example, Bitcoin* (Feb. 19, 2018), [https://taxes.gov.il/About/SpokesmanAnnouncements/Pages/Ann_190218_1.aspx](https://taxes.gov.il/About/SpokesmanAnnouncements/Pages/Ann_190218_1.aspx).

630 *Id.*


December 1, 2017, Japan’s National Tax Agency released a circular stating that income earned from virtual currency is treated as miscellaneous income rather than capital gains, and thus is subject to the potentially higher taxes on aggregate income.\textsuperscript{634} During the 2018 tax season, Japanese cryptocurrency investors paid 15-55\% on their virtual currency profits.\textsuperscript{635} By contrast, the top bracket is charged only 20\% for income derived from foreign exchange or stock market trading.\textsuperscript{636}

\textbf{South Africa:} On April 6, 2018, the South African Revenue Service (SARS) announced it will be treating cryptocurrencies as “assets of intangible nature,” not as traditional currencies. Thus, cryptocurrencies will be subject to the existing income and capital gain tax rules of South Africa.\textsuperscript{637} SARS seems not to have determined whether gains from trading cryptocurrency are subject to income tax or capital gains tax.\textsuperscript{638}

\textbf{Australia:} In Australia, transacting with cryptocurrencies is “akin to a barter arrangement, with similar tax consequences.\textsuperscript{639} Any financial gains made from selling cryptocurrencies will be subject to capital gain tax and must be reported to the Australian Taxation Office.\textsuperscript{640} In addition, cryptocurrencies may be considered assets for capital gains tax purposes, with the guidance stating: “Where you use bitcoin to purchase goods or services for personal use or consumption, any capital gain or loss from disposal of the bitcoin will be disregarded (as a personal use asset) provided the cost of the bitcoin is $10,000 or less.”\textsuperscript{641}

5.5 International Anti-Money Laundering Laws That Affect Virtual Currencies

Several countries have implemented AML regulations specific to virtual currencies or applied existing AML regulations to blockchain technology.

\textbf{Canada:} In 2014, the Governor General of Canada gave royal assent to Bill C-31, amending the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (2001).\textsuperscript{642} The

\begin{itemize}
  \item \textsuperscript{635} \textit{Id}.
  \item \textsuperscript{636} \textit{Id}.
  \item \textsuperscript{637} Press Release, \textit{South Africa Revenue Services, SARS’S Stance on the Tax Treatment of Cryptocurrencies} (Apr. 6, 2018), \url{http://www.sars.gov.za/Media/MediaReleases/Pages/6-April-2018---SARS-stance-on-the-tax-treatment-of-cryptocurrencies-.aspx}.
  \item \textsuperscript{638} \textit{Id}.
  \item \textsuperscript{640} \textit{Id}.
  \item \textsuperscript{641} \textit{Id}.
\end{itemize}
amendments provide that companies “dealing in virtual currencies” are “money service businesses” for AML purposes, and must register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), implement compliance programs, retain prescribed records, report suspicious or terrorist-related property transactions, and determine if any of their customers are “politically exposed persons.” The law applies not only to businesses dealing in virtual currency that operate within Canada but also to those operating outside the country who direct services at persons or entities in Canada.

**European Union:** On July 5, 2016, the European Commission submitted a proposal to amend its Fourth Anti-Money Laundering Directive (AMLD). This amendment brings custodian wallet providers and virtual currency exchange platforms within the scope of the AMLD, requiring them to meet due diligence requirements and implement policies and procedures to detect, prevent, and report money laundering and terrorist financing. The amendment defines ‘virtual currency’ as “a digital representation of value that is not issued by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.” The European Parliament adopted the text in a plenary session on April 19, 2018 and published it in the *Official Journal of the European Union* on June 19, 2018.

**Switzerland:** In 2014, Switzerland’s financial-markets regulator, the Swiss Financial Market Supervisory Authority (FINMA) released a report on virtual currencies. In it, the Federal Council concluded that professional trading in virtual currencies and the operation of trading platforms in Switzerland generally come under the scope of the Anti-Money Laundering Act.

---


644 Bill C3-1, *supra* note 642, at §256(2).


647 *Id.*


(AMLA)\textsuperscript{650} and thus trigger a range of due diligence obligations.\textsuperscript{651} These include verifying the identity of the contracting party and establishing the identity of the beneficial owner.\textsuperscript{652}

On February 16, 2018, FINMA issued guidelines explaining how ICOs would be regulated within the country.\textsuperscript{653} The guidelines stated that currently, there are no ICO-specific regulations, nor is there relevant case law, or consistent legal doctrine.\textsuperscript{654} In addition, the guidelines identify four categories of digital assets: payment tokens, utility tokens, asset tokens, and hybrid tokens.\textsuperscript{655} Payment tokens\textsuperscript{656} will be subject to regulation under the AMLA. Asset tokens,\textsuperscript{657} however, will not. Utility tokens\textsuperscript{658} will not be subject to the AMLA as long as “the main reason for issuing the tokens is to provide access rights to a non-financial application of blockchain technology.” Lastly, hybrid tokens\textsuperscript{659} may be subject to the AMLA if it possesses any characteristic of a utility token. Additionally, “the exchange of cryptocurrency for fiat money or a different crypto currency” will also fall under the purview of the AMLA.\textsuperscript{660} FINMA advised that each case will be “decided on individual merits.”\textsuperscript{661}

\textsuperscript{650} The AMLA generally applies to “financial intermediaries,” who are defined as natural and legal persons who accept or hold deposit assets for third parties or who assist in the investment or transfer of such assets on a professional basis. Geldwäschereigesetz [GwG] [Anti-Money Laundering Act] [AMLA], Oct. 10, 1997, SR 955.0, art. 2, para. 1, let. a, art 2, para. 3, \url{https://www.admin.ch/opc/de/classified-compilation/19970427/201601010000/955.0.pdf}.

\textsuperscript{651} Federal Council, \textit{supra} note 649.

\textsuperscript{652} AMLA, \textit{supra} note 650 at arts. 3, 4.


\textsuperscript{654} \textit{Id.} at pg. 3, Sec. 3.

\textsuperscript{655} \textit{Id.} at pg. 3, Sec. 3.1.

\textsuperscript{656} Payment tokens “synonymous with cryptocurrencies and have no further functions or links to other development projects. Tokens may in some cases only develop the necessary functionality and become accepted as means of payment over a period of time.”

\textsuperscript{657} Asset tokens “represent assets such as participants in real physical underlyings, companies, or an entitlement to dividends or interest payments. In terms of economic function, the tokens are analogous to equities, bonds or derivatives.”

\textsuperscript{658} Utility tokens “are intended to provide access digitally to an application or service.”

\textsuperscript{659} Hybrid tokens contain features of more than one of the above categories.


\textsuperscript{661} \textit{Id.}
On August 30, 2018, FINMA released a virtual currencies fact sheet stating that “some trading activities with virtual currencies require a banking license and involve ongoing monitoring by FINMA.”\(^{662}\) The fact sheet goes on to specify that the same requirements apply to “providers who lodge virtual currency holdings from customers in “wallets” and manage accounts for them.”\(^{663}\) However, “no banking license is required if virtual currency holdings are transferred only for secure safekeeping purposes and so long as each blockchain-based deposit can be attributed to an individual customer at all times.”\(^{664}\)

**Estonia:** On April 11, 2016, the Supreme Court of Estonia determined that a virtual currency exchange service is a provider of alternative means of payment under the country’s Money Laundering and Terrorist Financing Prevention Act.\(^{665}\)

Thereafter, on November 27, 2017, the Estonian parliament, Riigikogu, passed a new version of the Anti-Money Laundering Act and Terrorism Finance Act, replacing the former, vague definition of “virtual currency.”\(^{666}\) In addition, the law defined ‘cryptocurrency businesses’ as “providers of a service of exchanging a virtual currency against a fiat currency” and “providers of a virtual currency wallet service.”\(^{667}\) Any providers falling within this definition are subject to Estonia’s AML law.\(^{668}\) Finally, the law clarifies that in order to obtain a cryptocurrency exchange license, an application must be filed with the Register of Economic Activities.\(^{669}\)

---


\(^{663}\) Id.

\(^{664}\) Id.

\(^{665}\) *Appeal of Otto Albert de Voogd in Cassation*, No. 3-3-1-75-15 (Apr. 11, 2016), [https://www.riigikohus.ee/lahendid?asjaNr=3-3-1-75-15](https://www.riigikohus.ee/lahendid?asjaNr=3-3-1-75-15). As the Supreme Court of Estonia clarified, a “provider of alternative means of payment” is a person who, in the course of his economic or professional activities, buys, sells, or contracts funds that are financially valued by means of a communication, transfer, or clearing system that can be used to fulfill financial obligations or which can be exchanged between the current currency but not a credit or financial institution within the meaning of the Credit Institutions Act.

\(^{666}\) Under the law, a virtual currency is defined as “a value represented in the digital form, which is digitally transferable, preservable or tradeable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds…”; Rahapesu Ja Terrorismi Rahastamise Tõkestamise Seadus [Money Laundering and Terrorist Financing Prevention Act], Riigi Teataja [Official Gazette] RT I (Nov. 27, 2017), Sec. 3, [https://www.riigiteataja.ee/akt/117112017002](https://www.riigiteataja.ee/akt/117112017002) (in Estonian), English translation *available at* [https://www.riigiteataja.ee/en/eli/517112017003/consolide](https://www.riigiteataja.ee/en/eli/517112017003/consolide).

\(^{667}\) Id. at Ch. 1, Sec. 3.

\(^{668}\) Id.

\(^{669}\) Id. at Ch. 8.
Australia: In December 2017, Australia passed the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2017.670 The law requires “providers of registrable designated remittance services or registrable remittance network services” to register with the Australian Transaction Reports and Analysis Centre (AUSTRAC).671 AUSTRAC will compel exchanges to sign up to a Digital Currency Exchange Register while enacting KYC and transparency protocols in order to mitigate terrorist activities and money laundering.672 Exchanges are required to report any suspicious account activity or certain international transactions, and maintain customer identification records for seven years.673

Malaysia. On February 27, 2018, the Bank of Negara Malaysia issued guidelines entitled Anti-Money Laundering and Counter Financing of Terrorism (AML/CTF) – Digital Currencies (Sector 6).674 The guidelines highlight that “any person offering services to exchange digital currencies either from or to fiat money, or from or to another digital currency” is subject to obligations under the AMLA as a reporting institution.675 The Bank of Negara also included that reporting institutions were required to perform enhanced customer due diligence where the ML/TF risks are assessed as higher-risk.676

5.6 Regulatory Sandboxes

In recent years, several countries have created “regulatory sandboxes” to facilitate technological innovation. Regulatory sandboxes act as restricted playgrounds that allow FinTech businesses (companies that develop new technology for the financial services industry) to test innovative products and business models in a controlled environment with legal restrictions relaxed.677

671 Id. at Part 2, Sec. 4.
672 Id. at Part 6A.
675 Id.
676 Id.
677 Although FinTech firms participating in a sandbox operate under relaxed regulations for the experiment, they must still comply with laws and regulations outside the jurisdiction of the government agency that provides the sandbox. Thus, for example, participants in the Australian Securities and Investments Commission’s sandbox must comply with anti-money laundering laws. ASIC, Regulatory Sandbox, http://asic.gov.au/for-business/your-business/innovation-hub/regulatory-sandbox/ (last updated Aug. 23, 2018); see also Dan Cummings, Regulatory Sandboxes: A Practice For Innovation That Is Trending Worldwide, ETHNews (Feb. 28, 2017);
**Australia:** A business seeking to offer financial services (e.g., providing financial product advice or making a market for a financial product) or to engage in credit activities must obtain an Australian financial services or credit license from the Australian Securities and Investments Commission (ASIC).678 Businesses that intend to develop blockchain technology products for the financial services sector must also comply with this regulatory framework.679 In order to foster innovation, in 2016, ASIC created a regulatory sandbox for eligible FinTech businesses to test specified services,680 without requiring them to obtain an Australian financial services license or credit license.681 Eligible businesses must meet various conditions, including having less than 100 retail clients, testing products for no more than 12 months, satisfying insurance and disclosure requirements, and having dispute resolution processes.682

**Bahrain:** On June 14, 2017, the Central Bank of Bahrain created a regulatory sandbox to strengthen the nation’s position as the Fintech and financial services hub in the Persian Gulf region.683 Testing is limited to a nine-month period, with a maximum extension of three months.684 To qualify, the FinTech solution must be innovative (i.e., different from existing financial solutions) and provide identifiable benefits to customers.685 Eligible businesses must meet certain conditions, including satisfying disclosure and risk mitigation requirements, and complying with AML and KYC requirements.686

---


681 ASIC, supra note 677.


684 Id.


686 Id.
Canada: On February 23, 2017, the Canadian Securities Administrators (CSA)\textsuperscript{687} launched a regulatory sandbox initiative that allows firms seeking to offer innovative FinTech products in Canada to register and obtain exemptions from securities laws requirements.\textsuperscript{688} Businesses that are potentially eligible for these exemptions include cryptocurrency or distributed ledger technology-based ventures (e.g., companies with proposed ICOs).\textsuperscript{689} Interested businesses must file an application with their local securities regulators, who then refer the application to the CSA.\textsuperscript{690} The CSA then reviews the application, and determines the limits and conditions for the business to participate in the sandbox.\textsuperscript{691} As of September 2018, eight companies had been authorized to participate in the CSA Regulatory Sandbox.\textsuperscript{692}

Hong Kong: On September 6, 2016, the Hong Kong Monetary Authority (HKMA) launched the Fintech Supervisory Sandbox, which is only offered to established banks and their partnership technology firms (and not start-up FinTech firms) seeking to explore FinTech initiatives in a controlled environment without the need to comply with full HKMA regulatory requirements.\textsuperscript{693} Authorized banks must comply with various conditions, including implementing customer protection measures and risk management controls.\textsuperscript{694} As of July 2018, 33 new technology products had been tested in the sandbox, 26 of which had been completed with the products subsequently rolled out to market.\textsuperscript{695}

\textsuperscript{687} The Canadian Securities Administrators is an umbrella organization of Canada’s provincial and territorial securities regulators that seeks to coordinate and harmonize regulations for the Canadian capital markets.


\textsuperscript{690} Canadian Sec. Admins., \textit{supra} note 688.

\textsuperscript{691} \textit{Id}.


\textsuperscript{694} Letter from Arthur Yuen, \textit{supra} note 693.

\textsuperscript{695} Hong Kong Monetary Authority, FinTech Supervisory Sandbox (FSS), https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech-supervisory-sandbox.shtml (last updated Nov. 12, 2018).
**Malaysia:** On October 18, 2016, Bank Negara Malaysia, the Malaysian central bank, issued its Financial Technology Regulatory Sandbox Framework. An applicant must satisfy various eligibility criteria, including demonstrating that its product or service is innovative, demonstrating that it has plans for deployment after testing, identifying risks, and proposing safeguards. As of December 2018, seven companies were undergoing testing in the regulatory sandbox.

**Singapore:** On November 16, 2016, the Monetary Authority of Singapore (MAS), the nation’s central bank, published its regulatory sandbox guidelines. The MAS sandbox allows FinTech firms to experiment with innovative financial services and products in an environment with relaxed MAS regulatory requirements. Applicants must have a time limit for the testing, a customer limit, a dispute resolution process, a risk management plan, and customer disclosures. As of August 2018, four companies were actively participating in the sandbox.

Additionally, on June 28, 2017, MAS and the Danish Financial Supervisory Authority (Danish FSA) signed a FinTech Co-operation Agreement, which aims to assist FinTech companies in Singapore and Denmark to expand into each other’s market. The agreement allows both MAS and Danish FSA to refer FinTech companies to their counterpart, explore joint projects together, and share information on emerging market trends and their impact on regulation.

---


701 Id.


704 Id.
**Switzerland**: In August of 2017, the Swiss Federal Council amended the Swiss Federal Banking Ordinances to ease the Swiss regulatory framework for providers engaged in innovative FinTech. Part of the ordinance implemented a sandbox where FinTech companies are allowed to accept deposits from the public up to a maximum amount of CHF 1 million without a banking license so long as the assets are neither invested nor interest-bearing. The companies can then use the money to test the viability of their business models before expanding their activities and applying for a banking license.

**Thailand**: In December 2016, the Bank of Thailand, the country’s central bank, announced a regulatory sandbox for financial institutions, FinTech firms, and other technology firms seeking to test innovations for lending, payment, and other types of transactions that fall within the bank’s supervisory authority, including the use of blockchain technology to facilitate international money transfers. Participants are required to maintain measures for good corporate governance, privacy, and security. As of September 2017, four companies had been approved by the central bank for participation in the sandbox, including three companies applying blockchain technology to letters of guarantee and cross-border transfers.

**United Kingdom**: In 2015, the UK’s Financial Conduct Authority (FCA), which regulates the country’s financial services, launched a regulatory sandbox that offers a supervised environment for firms to operate under a restricted authorization, regulatory guidance, and waiver of rules or no enforcement letters for the duration of the testing. To be eligible, the product or service must be innovative (i.e., ground-breaking or significantly different from current offerings), benefit consumers, not easily fit within the current regulatory framework, and be ready for

---


706 Id.

707 Id.


710 Corbett, *supra* note 708.


testing. The sandbox has finished three regulatory rounds and by July of 2018 had accepted 29 FinTech companies into round four.

**Netherlands:** In June of 2016, the Dutch Central Bank (DNB) and the Netherlands Authority for Financial Markets (AFM) created a Dutch regulatory sandbox that provides an environment in which “tailor-made solutions” are created to safely test innovative products and business models. Any financial institution, whether aspiring or authorized, is eligible to join. The applicant’s innovative concept must be currently hindered by policies, rules or regulations with which the applicant cannot reasonably comply. Additionally, the applicant must show that adequate measures and procedures are in place in order to protect the applicant and interests of the shareholder.

**Brunei:** On February 27, 2017, the Autoriti Monetari Brunei Darussalam (AMBD) announced a regulatory sandbox to facilitate the development of financial technology. The guidelines state: “the movement towards being an E-Payment economy is also a focus, i.e. moving away from being paper-based in favour [sic] of electronic methods.” The sandbox will allow any financial institution or FinTech company to experiment with new products, services, and business models.

**Japan:** On September 21, 2017, the Financial Services Agency (FSA) established a FinTech sandbox to address concerns regarding compliance of experimental FinTech projects. A team within FSA will provide assistance to FinTech companies that are introducing novel FinTech

---


716 *Id.*

717 *Id.*


719 *Id.*
experiments. Applicants submit an application, and the FSA investigates to determine whether to provide the company assistance.

**Indonesia:** In December of 2017, Indonesia’s Central Bank, the Bank of Indonesia (BI), released new guidelines for the FinTech sector, by introducing a regulatory sandbox that allows FinTech companies to test new products under BI-controlled supervision. To join, FinTech companies must register with BI by providing information such as a deed of establishment, ownership structure, and a description of the company’s FinTech products or services. Once registered, applicants are assessed by BI, and a list of those accepted is published on its website. Thereafter, the FinTech companies are required to submit details on relevant transactions as well as their products/services, financial status, and management/ownership.

**Abu Dhabi:** On May 10, 2016, the Financial Services Regulatory Authority (FSRA) of Abu Dhabi Global Market (ADGM) announced a regulatory sandbox that would be available to companies developing innovative technologies in the financial services sector. FSRA guidelines indicate that FinTech companies will be able to participate in the sandbox for two years and may use this time to develop, test and launch products and services in a controlled environment. The sandbox adopted a “blank sheet” approach, meaning that FinTech companies are not subjected to a full set of rules; instead, the FSRA creates a set of rules customized to the business model, technology deployed and risk profile of the FinTech company. To be eligible, participants must be FinTech start-ups or existing financial institutions with FinTech products or services, the project must promote novel innovation and growth, the project must be advanced enough to mount a live test during the two-year period, and the applicant must establish test parameters, milestones,

---


723 *Id.*

724 *Id.*


726 *Id.*

727 *Id.*
safeguards, and an exit strategy for consumers. On February 26, 2018, the ADGM announced that it is opening applications for the third phase of this regulatory sandbox.

**Dubai:** In May 2017, the Dubai Financial Services Authority (DFSA) invited FinTech firms to apply for an Innovation Testing License (ITL), which will allow the companies to develop and test concepts for six to twelve months in a regulated environment. To qualify, firms must demonstrate that the business model, product or service is innovative and brings a new benefit to customers. If the product or service is ready for testing, applicants must provide a regulatory test plan with examples delineating how the company intends to start its business at the end of the test period.

**Russia:** On April 19, 2018, the Central Bank of Russia announced the launch of a regulatory sandbox. Any organization that has developed or plans to use an innovative financial service may initiate a pilot in the regulatory sandbox. In its application, the FinTech firm must provide information on the advantages of the use of the new product as well as its potential impact on the financial market.

**Taiwan:** On January 21, 2018, the President of Taiwan promulgated the Financial Technology Innovations and Experiments Act. FinTech firms that pass an assessment to use the sandbox can bypass certain regulations. The committee that monitors the Act will be comprised of both experts from the private sector and representatives from government agencies. The sandbox is expected to last anywhere from 18 to 36 months and is open to all natural persons and

---


731 *Id.*

732 *Id.*


735 *Id.*

legal entities. Applicants must demonstrate that the product or service is innovative, that it promotes financial efficiency, reduces costs, and benefits customers, and that measures exist to protect participating consumers from potential harm.

**Global Financial Innovation Network**: On August 8, 2018, the Financial Conduct Authority of the United Kingdom announced the creation of the Global Financial Innovation Network (GFIN). Sandbox participants include but are not limited to the Abu Dhabi Global Market, the Australian Security & Investments Commission, the Bureau of Consumer Financial Protection, the Hong Kong Monetary Authority, and the Ontario Securities Commission. GFIN seeks to “(1) act as a network of regulators to collaborate and share experience of innovation in respective markets, including emerging technologies and business models; (2) provide a forum for joint policy work and discussions; and (3) provide firms with an environment in which to trial cross-border solutions.”

---

737 *Id.*


740 *Id.*

741 *Id.*
Chapter 6

6 Anti-Money Laundering and Countering Terrorism Financing

Money laundering is the act of transferring illegally obtained money through legitimate persons or accounts so that its original source cannot be traced.\footnote{Money-Laundering, Black's Law Dictionary (4th pocket ed. 2011).} Plainly put, money laundering aims to make ill-gotten funds appear legitimate. There are many reasons why criminals launder money, including to “clean” cash from illegal businesses, to evade taxes, and to fund illegal operations, such as terrorist operations or drug trafficking. The United Nations Office on Drugs and Crime estimates that each year 2-5% of global GDP, or about $800 billion to $2 trillion, is laundered worldwide.\footnote{U.N. Office on Drugs and Crime, Money-Laundering and Globalization, https://www.unodc.org/unodc/en/money-laundering/globalization.html (last visited Nov. 20, 2018).} In 2015, it was estimated that $300 billion is laundered annually in the United States alone.\footnote{U.S. Dept. of the Treasury, National Money Laundering Risk Assessment 2015, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%20%E2%80%93%2006-12-2015.pdf (last visited Nov. 20, 2018).}

Terrorist financing is the “solicitation, collection or provision of funds with the intention that they be used to support terrorist acts or organizations.”\footnote{Int’l Monetary Fund, Anti-Money Laundering/Combating the Financing of Terrorism https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm (last visited Nov. 15, 2018).} Persons engaged in terrorist financing seek to conceal not only the source of the funds but also the criminal activity being supported.\footnote{Id.} Money laundering is one of the most common methods of doing just that.\footnote{See, e.g., U.S. Dep’t of State, Country Reports on Terrorism 2015 (Jun. 2, 2016), https://www.state.gov/documents/organization/258249.pdf.}

6.1 The Basics of Money Laundering

entails depositing or “placing” the funds with a financial institution, such as a bank. The illegal funds can also be exchanged for other currency or used to purchase other financial instruments, like money orders or securities. This is the riskiest step, if the transaction triggers a suspicious activity alert pursuant to a financial institution’s anti-money laundering (AML) policies, the institution will file a Suspicious Activity Report (SAR) with the Financial Crimes Enforcement Network (“FinCEN”), which could lead to a criminal investigation by federal authorities. To make the funds appear legitimate, they can be broken up into smaller amounts and deposited with different financial institutions.

In the second step, the funds are “layered” by constantly transferring them through multiple legitimate accounts to conceal the illegal source. This can be done by moving the funds between different accounts and financial institutions, or by purchasing and reselling high-priced items, securities, or real estate. These transfers are designed to make the funds difficult to trace as an investigator would need to follow the trail through multiple financial institutions or transactions to discover the funds’ origin.

In the final step, integration, the funds that were placed in the financial system and layered to obscure their source are returned to the criminal in legitimate form for use in normal business or personal transactions. These additional normal transactions further disguise the illegality of the funds by “providing a plausible explanation for the source of the funds.”

6.2 Use of Virtual Currency in Money Laundering

The cryptographic nature of virtual currency makes it susceptible to bad actors. In the early years of bitcoin, the unfamiliarity of law enforcement and regulators with the technology

---


749 Id.

750 Schott, supra note 748.


752 Id.

753 Id.

754 ACAMS, supra note 748, at 15-18.

755 Id.

756 Id.


allowed criminals to take advantage of the anonymity afforded by virtual currency and its relatively quick, largely untraceable money-transfer capability to launder large amounts of criminal proceeds.

Typically, wrongdoers using virtual currency to launder money do so in either the placement or layering phases. The wrongdoer takes criminal proceeds in cash and exchanges them directly for virtual currency, likely through an exchange site, in several different transactions to obscure the source of the funds. To layer the funds and minimize suspicion, purchases are made in small transactions. After layering, the wrongdoer can then exchange the virtual currency for fiat currency, enabling use of the funds as if they were legitimate and derived from lawful transactions. Within the past few years, U.S.-based centralized virtual currency exchange sites such as Coinbase and Gemini have made significant efforts to comply with AML laws and know your customer (KYC) regulations. However, there are many centralized exchanges in countries with less strict, or relatively non-existent, AML/KYC regulations, as well as decentralized exchanges that are difficult to monitor.

While media coverage has focused on the potential of virtual currency to facilitate money laundering activity, increased regulation has helped cryptocurrency shed some of the criminal stigma associated with its anonymous nature. This chapter discusses the current U.S. federal AML framework and examines how regulators may approach this new technology.


761 Id.


763 European Cybercrime Centre, supra note 759.


6.3 Federal AML Framework

To combat money laundering, the federal government has enacted various laws over the past five decades requiring financial institutions to take substantial action to safeguard against illicit activity. These requirements have forced financial institutions to implement procedures for auditing their clients’ transactions to ensure they are not facilitating money laundering activities. Nevertheless, over the years, many large financial institutions have paid heavy fines for failure to comply with AML laws.  

6.3.1 Bank Secrecy Act of 1970 and PATRIOT Act

The Bank Secrecy Act of 1970 (BSA) was the first sweeping federal statute enacted to prevent money laundering and other illegal activities, such as tax evasion and terrorist financing, through the imposition of recordkeeping and reporting requirements on financial institutions. The federal agency with primary authority to administer and enforce the requirements of the BSA is the Financial Crimes Enforcement Network (FinCEN). FinCEN was originally created in 1990 to provide intelligence and analytics support to the government in identifying, investigating, and prosecuting domestic and international financial crimes, including money laundering. Other federal regulatory agencies, such as the Office of the Comptroller of the Currency and the

---


770 FinCEN was originally created by Treasury Order 105-08, U.S. Dept. of Treasury, Financial Crimes Enforcement Network, https://www.treasury.gov/about/history/Pages/fincen.aspx (last updated Nov. 13, 2010).
Securities and Exchange Commission, are also authorized to examine financial institutions for compliance.  

Following the September 11 attacks, in October 2001, Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (PATRIOT Act). Among other things, the PATRIOT Act amended the BSA to expand measures to help prevent money laundering, including expanding the required AML procedures and prohibiting financial institutions from doing business with foreign shell banks. The PATRIOT Act also expanded FinCEN’s reach, putting the agency in charge of the central collection, analysis, and dissemination of data reported under FinCEN’s regulations in order to combat money laundering and terrorism financing.

### 6.3.1.1 Scope

To assist law enforcement agencies with identifying the source, volume, and movement of currency into and out of the United States, the BSA imposes extensive reporting and recordkeeping obligations on financial institutions and persons who engage in certain transactions. A “financial institution” is defined to include, among other things, an insured bank, a commercial bank or trust company, a credit union, a broker or dealer in securities or commodities, a money services business, and any business engaged in activities deemed similar by the Secretary of the Treasury.


775 The statute defines “persons” to include corporations, companies, and other entities. 31 U.S.C. § 5312(a)(5); 1 U.S.C. § 1.

776 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).

777 The regulations define “money service business” as a “person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in one or more of the following activities: dealer in foreign exchange; check casher; issuer or seller of traveler’s checks or money orders; provider of prepaid access; money transmitter; U.S. Postal Service; or seller of prepaid access. 31 C.F.R. § 1010.100(ff). The regulations further define “money transmitter” to include a person that provides money transmission services (“the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.”). Id.
Treasury, and any business “designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.”778

6.3.1.2 AML Requirements

The BSA requires financial institutions to file a Currency Transaction Report (CTR)779 with FinCEN for every transaction involving more than $10,000 in cash within 15 days of the transaction.780 Also, when a financial institution has facts demonstrating possible illegal activity, it is required to file a SAR781 with FinCEN within 30 days of the initial detection of facts that would constitute a basis for filing a SAR.782

The BSA also requires persons who transport currency or other monetary instruments in excess of $10,000 into or out of the United States to file a report with the U.S. Customs officer at the port of entry or departure within 15 days of receipt of the currency or monetary instruments.783 FinCEN also requires annual reports from persons who have a financial interest in a bank, securities, or other financial account in a foreign country.784

Additionally, the BSA imposes numerous internal recordkeeping requirements on financial institutions,785 including requirements that they maintain the original or a copy of: (1) a record of each extension of credit in excess of $10,000; (2) a record of each request or instruction regarding a transaction resulting in the transfer of currency or monetary instruments in excess of $10,000 to or from a person or account outside the United States; (3) a record of each request or instruction given to another financial institution or person within or without the United States regarding a transaction intended to result in the transfer of currency or monetary instruments in excess of $10,000 to or from a person or account outside the United States; and (4) a record of any other information ordered by the Secretary of the Treasury.786 Nonbank financial institutions are also required to maintain records for each transmittal order exceeding $3,000.787

778 31 U.S.C. § 5312(a)(2)(Z); 31 C.F.R. § 1010.100(t).
781 For more information on SARs, see https://www.fincen.gov/frequently-asked-questions-regarding-fincen-suspicious-activity-report-sar.
782 31 U.S.C. § 5318(g); 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, 1030.320.
784 31 C.F.R. §§ 1010.306(c), 1010.350.
785 31 C.F.R. § 1010.400, et seq.
786 31 C.F.R. § 1010.410(a)-(d).
787 31 C.F.R. § 1010.410(e).
In addition, FinCEN requires domestic financial institutions to adopt AML and customer identification programs. 788 For example, money service businesses are required to “develop, implement, and maintain an effective anti-money laundering program,” which is defined as “one that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities.” 789 The program must be “commensurate with the risks posed by the location and size of, and the nature and volume of the financial services provided by, the money services business,” and have at minimum: (1) policies and procedures to assure compliance with the regulation, including procedures for verifying customer identification, filing reports, retaining records, and responding to law enforcement requests; (2) a designated compliance officer; (3) training and education for appropriate personnel; and (4) procedures for independent review of the program. 790

In 2006, following several instances where large financial institutions were assessed civil penalties for noncompliance with the BSA, FinCEN provided guidance on best practices for maintaining a strong BSA/AML compliance program. 791 Additionally, in 2007, the Federal Financial Institutions Examination Council (FFIEC) 792 released the revised BSA/AML Examination Manual, which “reflects the ongoing commitment of the federal and state banking agencies and [FinCEN] to provide current and consistent guidance on risk-based policies, procedures, and processes for banking organizations to comply with the BSA and safeguard operations from money laundering and terrorist financing.” 793 Best practices, as outlined in the 2006 FinCEN guidance and described in the BSA/AML Examination Manual, suggest that financial institutions: (1) develop a comprehensive risk assessment; 794 (2) develop appropriate


789 31 C.F.R. § 1022.210(a).

790 31 C.F.R. § 1022.210(b)-(d).


792 The FFIEC is an interagency body established in March 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA). Its purpose is to prescribe uniform principles, standards, and report forms, and to promote uniformity in the supervision of financial institutions. FFIEC, About the FFIEC, https://www.ffiec.gov/ (last updated Oct. 4, 2018).


policies and procedures to address the financial institution’s risk profile;\textsuperscript{795} (3) have adequate monitoring programs;\textsuperscript{796} (4) implement strong training programs;\textsuperscript{797} (5) conduct thorough independent testing;\textsuperscript{798} and (6) hire qualified employees to oversee day-to-day operations.\textsuperscript{799}

6.3.1.3 Penalties

Financial institutions that violate the BSA are subject to criminal and civil penalties, as well as forfeiture\textsuperscript{800} and injunctions.\textsuperscript{801} For willful violations of the BSA or its implementing regulations, or for structuring transactions to evade BSA recordkeeping and reporting requirements, a violator faces a maximum fine of $250,000, five years’ imprisonment, or both.\textsuperscript{802} For violations of the BSA or its implementing regulations while violating another federal law or engaging in a pattern of illegal activity, a violator faces a maximum fine of $500,000, ten years’ imprisonment, or both.\textsuperscript{803} For violations of certain other provisions of the BSA – i.e., Sections 5318 (which concerns banking involving foreign persons or foreign shell banks) and 5318A (special measures related to foreign jurisdictions, foreign financial institutions, international transactions, or certain types of accounts – a violator faces a maximum fine of $1,000,000).\textsuperscript{804}

FinCEN may also institute civil actions to recover civil penalties for violations of the BSA, including for negligent violations.\textsuperscript{805} The amount of the penalty varies with the nature of the violation. For example, a negligent violation subjects one to a penalty of not more than $500, while a willful violation subjects one to a penalty of either the amount involved in the transaction or $25,000, whichever is greater.\textsuperscript{806}

\footnotesize
\textsuperscript{795} \textit{Id.}
\textsuperscript{797} \textit{Id.}
\textsuperscript{798} \textit{Id.}
\textsuperscript{800} 31 U.S.C § 5317.
\textsuperscript{801} 31 U.S.C § 5320.
\textsuperscript{802} 31 U.S.C § 5322(a).
\textsuperscript{803} 31 U.S.C § 5322(b); 31 U.S.C. 5324(d).
\textsuperscript{804} 31 U.S.C § 5322(d).
\textsuperscript{805} 31 U.S.C § 5321.
\textsuperscript{806} \textit{Id.}
6.3.1.4 FinCEN Guidance

Over the past several years, FinCEN has issued guidance with respect to virtual currency transactions and virtual currency-related businesses. Pursuant to FinCEN regulations, the term “financial institutions” encompasses “money service businesses” (MSB), which includes a “money transmitter.” A “money transmitter” is defined as a person who “[accepts] currency, funds, or other value that substitutes for currency from one person [and] transmit[es] currency, funds, or other value that substitutes for currency to another location or person by any means,” or who engages in the transfer of funds.

FinCEN has determined that an administrator or exchanger of decentralized and centralized virtual currency falls within the ambit of the BSA:

[A]n administrator or exchanger of convertible virtual currencies that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency in exchange for currency of legal tender or another convertible virtual currency for any reason (including when intermediating between a user and a seller of goods or services the user is purchasing on the user’s behalf) is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person.

According to FinCEN’s guidance, an administrator is a person or entity in control of the repository of a centralized virtual currency. Examples include WebMoney, a global payment settlement system where transactions are made using a centralized virtual currency called WM, and Linden Lab, a massive multiplayer online game that uses a centralized virtual currency called Linden Dollars. An exchanger is a person or entity that either accepts fiat currency and transmits its value in virtual currency to another location or person, or accepts virtual currency, whether centralized or decentralized, and “transmits it to another person as part of the acceptance and

---

808 31 C.F.R. § 1010.100(t).
809 31 C.F.R. § 1010.100(ff).
810 31 C.F.R. § 1010.100(ff)(5).
811 FinCEN has defined an “administrator” of virtual currency as “a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.” FIN-2013-G001. FinCEN has further defined an “exchanger” of virtual currency as “person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency.” FIN-2013-G001.
812 FIN-2014-R001.
813 FIN-2013-G001.
814 See generally Section 1.1.4.
815 See generally Section 1.1.5.
transfer of currency, funds, or other value that substitutes for currency.” An exchanger can be a virtual currency exchange or a company that accepts fiat currency from a consumer and transmits its equivalent in virtual currency to a merchant.

FinCEN has also concluded that a person who uses virtual currency to buy goods or services for the user’s own benefit is not a money transmitter so long as the virtual currency is transmitted to the seller of the goods or services and not to a third party as directed by the seller. Additionally, a company that converts virtual currency to fiat currency for its own benefit is a user and not a money transmitter. The method by which a user obtains the virtual currency (e.g., through mining or purchasing) is immaterial to the determination of whether a user is a money transmitter under the BSA.

On March 6, 2018, FinCEN published a letter, which had been previously sent to U.S. Senator Ron Wyden, clarifying its interpretation of current laws (e.g., BSA and AML) as they relate to ICOs. The letter states that a developer that sells convertible virtual currency, including in the form of ICO coins or tokens, in exchange for another type of currency is considered a money transmitter and must comply with AML/CFT requirements. Similarly, the letter also stated that an exchange which sells ICO coins or tokens – or which exchanges them for other virtual currency, fiat currency or other value – is also typically considered to be a money transmitter. The letter however, did acknowledge that “ICO arrangements vary” and that there are jurisdictional differences depending on the make-up of an ICO and its associated token.

### 6.3.1.5 FinCEN Enforcement Activity

Since issuing its guidance, FinCEN has pursued enforcement actions against several businesses in the crypto community for failure to register as MSBs or to comply with BSA requirements.

On May 5, 2015, FinCEN announced a civil monetary penalty of $700,000, against Ripple Labs, Inc., a virtual currency exchange, for violations of the BSA. Ripple Labs had failed to register with FinCEN and continued to act as an MSB despite the bureau’s 2013 guidance. Ripple

---

816 FIN-2013-G001.
817 FIN-2013-R011.
818 FIN-2013-R012.
819 FIN-2013-G001; FIN-2014-R001.
820 FIN-2014-R001.
821 FIN-2014-R001; FIN-2014-R007.
823 Id.
824 Id.
Labs had also failed to establish an AML program and to adopt policies to comply with its obligations under the BSA. Ripple Lab’s subsidiary, XRP, was registered with FinCEN but had failed to adopt an AML program and report suspicious transactions.  

On July 27, 2017, FinCEN announced penalties of $110 million against Russia-based virtual currency exchange BTC-e, and $12 million against one of its operators, Russian national Alexander Vinnik, for violating U.S. AML laws by failing to register as an MSB, failing to obtain customer information, and failing to report suspicious activity. BTC-e and Vinnik were also indicted for violations of 18 U.S.C. § 1956 and § 1957 for money laundering, engaging in unlawful monetary transactions, and operation of an unlicensed money transmitting business.

6.3.2 Money Laundering Control Act of 1986

Enacted in 1986, the Money Laundering Control Act (MLCA) was the first federal statute to criminalize money laundering. The MLCA consists of two sections: Section 1956, criminalizing the laundering of monetary instruments; and Section 1957, prohibiting monetary transactions in property derived from specified unlawful activity.

6.3.2.1 Section 1956

Section 1956 criminalizes three types of money laundering conduct: Subsection (a)(1) applies to domestic transactions, (a)(2) to international transactions, and (a)(3) to transactions conducted as part of a “sting” operation.

Section 1956(a)(1) prohibits a person from conducting or attempting to conduct a financial transaction where the property involved was derived from some statutorily specified unlawful activity and the person knows that it was illegally obtained. The statute defines “specified unlawful activity” to include numerous types of criminal activities, including racketeering activity, acts constituting a continuing criminal enterprise as defined under the Controlled Substances Act, kidnapping, murder, counterfeiting, and espionage.
specific underlying offense is not required. Prosecutors must also prove that the defendant acted with: (1) intent to promote further specified unlawful activities; (2) intent to evade taxation; (3) knowledge that the transaction was designed to conceal laundering of the proceeds; or (4) knowledge that the transaction was designed to avoid AML reporting requirements.

Section 1956(a)(2) criminalizes the international transportation or transmission of monetary instruments or funds. Prosecutors must establish that the defendant acted with either (1) intent to promote a specified unlawful activity; (2) knowledge that the purpose was to conceal laundering of the monetary instruments or funds; or (3) knowledge that the purpose was to avoid reporting requirements. For concealment and avoidance of reporting requirements, prosecutors must also show that the monetary instruments or funds were derived from specified unlawful activity.

Section 1956(a)(3) applies to undercover investigations, prohibiting financial transactions that the defendant believes involve the proceeds of a specified unlawful activity and are intended to (1) promote a specified unlawful activity, (2) conceal the source or ownership of the proceeds, or (3) avoid reporting requirements.

The statute defines “monetary instruments” as “(i) coin or currency of the United States or of any other country, travelers’ checks, personal checks, bank checks, and money orders, or (ii) investment securities or negotiable instruments, in bearer form or otherwise in such form that title thereto passes upon delivery.” Courts have interpreted the definition of “funds” to include virtual currencies. In United States v. Ulbricht, the government charged a website operator with participating in a money laundering conspiracy by operating a website that facilitated illicit transactions and used bitcoin as a payment system. The court found that bitcoin fell within the plain meaning of the term “funds” because it can “be either used directly to pay for certain

---


834 18 U.S.C. § 1956(a)(2); Doyle, supra note 833.


839 Id. At 570 (“‘Funds’ are defined as ‘money, often money for a specific purpose.’ … ‘Money’ is an object used to buy things.”) (quoting Cambridge Dictionaries Online).
things or can act as a medium of exchange and be converted into a currency which can pay for things.”

An individual convicted of violating Sections 1956(a)(1) or (a)(2) faces imprisonment for 20 years; a fine of $500,000 or twice the value of the property, monetary instruments, or funds involved in the violation, whichever is greater; or both. An individual who violates 1956(a)(3) faces a fine of $250,000 or twice the amount of the involved offense, whichever is greater; imprisonment for 20 years; or both. Civil penalties may also be assessed, and the proceeds or property involved in a Section 1956 offense may be forfeited.

### 6.3.2.2 Section 1957

Section 1957 criminalizes the spending or depositing of tainted money by prohibiting the use of criminally derived property (valued in excess of $10,000) in a monetary transaction. The government must prove that:

1. The defendant engaged or attempted to engage in a monetary transaction
2. In criminally derived property that is of a value greater than $10,000
3. Knowing that the property is derived from unlawful activity, and
4. In fact, derived from “specified unlawful activity.”

Prosecutors must also establish that the offense took place in the United States, or if it occurred outside the country, that the offender is a United States person as defined in 18 U.S.C. § 3077.

The use of criminally derived virtual currencies likely falls within the scope of Section 1957. A monetary transaction includes the deposit, withdrawal, transfer, or exchange of funds by or through a financial institution. While Section 1957 does not define “funds,” courts interpreting that term under Section 1956 have concluded that virtual currencies fall within its ordinary meaning because they can be used “to pay for certain things or can act as a medium of exchange.” Moreover, a virtual currency exchange qualifies as a “financial institution” under

---

840 Id.; see also United States v. Budovsky, No. 13cr368 (DLC), 2015 WL 5602853, at *13-14 (S.D.N.Y. Sept. 23, 2015) (adopting the Ulbricht court’s reasoning that virtual currencies are funds for purposes of Section 1956).


846 United States v. Sokolow, 91 F.3d 396, 408 (3d Cir. 1996) (quoting United States v. Johnson, 971 F.2d 562, 567 n.3 (10th Cir. 1992)).


849 Ulbricht, 31 F.Supp.3d at 570; see also Budovsky, No. 13cr368 (DLC), 2015 WL 5602853, at *13-14.
relevant provisions of both the Bank Secrecy Act and FinCEN regulations incorporated into the MLCA.\textsuperscript{850}

In contrast to Section 1956, a Section 1957 offense does not require intent to conceal or disguise for the scienter element to be satisfied. Under Section 1957, the government needs only prove that the defendant engaged in the transaction with knowledge that the subject property was the proceeds of any crime,\textsuperscript{851} not necessarily that the proceeds were derived from “specified unlawful activity.”\textsuperscript{852} The Government may also meet this burden with proof of willful blindness – i.e., “that a defendant was objectively aware of the high probability of the fact in question, and could have recognized the likelihood of illicit acts yet deliberately avoided learning the true facts.”\textsuperscript{853}

Violations of Section 1957 can result in a fine of $250,000 or twice the amount of the criminally derived property involved in the transaction; 10 years’ imprisonment; or both.\textsuperscript{854} Civil penalties may also be assessed,\textsuperscript{855} and the proceeds or property involved in a Section 1957 offense may be forfeited.\textsuperscript{856}

6.3.3 Prohibition of Unlicensed Money Transmitting Businesses

The Annunzio-Wylie Anti-Money Laundering Act of 1992 (18 U.S.C. § 1960) criminalizes the ownership or operation of unlicensed money transmitting businesses.\textsuperscript{857} Under the statute, “money transmitting” is broadly defined to include transfers by wire and check.\textsuperscript{858}

Section 1960 prohibits three types of unlicensed money transmitting businesses: (1) businesses that operate without a required state money transmitting license; (2) businesses that fail

\textsuperscript{850} See generally Section 6.3.1.4 and note 808.

\textsuperscript{851} United States v. Flores, 454 F.3d 149, 155 (3d Cir. 2006); United States v. Rice, 551 Fed. Appx 656, 662 n.4 (4th Cir. 2014) (“All the Government must prove is that the defendant knew that the property was obtained from some criminal offense.”); H.R. Rep. No. 855, 99th Cong., 2d Sess. 13 (1986) (“A person who engages in a financial transaction using the proceeds of a designated offense would violate [Section 1957] if such person knew that the subject of the transaction were the proceeds of any crime.”).

\textsuperscript{852} 18 U.S.C. § 1957(c).

\textsuperscript{853} United States v. Flores, 454 F.3d 149, 155 (3d Cir. 2006) (internal quotation marks and edits omitted).

\textsuperscript{854} 18 U.S.C. § 1957(b).

\textsuperscript{855} 18 U.S.C. § 1956(b).

\textsuperscript{856} 18 U.S.C. §§ 981, 982.

\textsuperscript{857} 18 U.S.C. § 1960(a) (“Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.”).

\textsuperscript{858} “Money transmitting” is the act of “transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier.” 18 U.S.C. § 1960(b)(2).
to comply with federal money transmitting business registration requirements; and (3) businesses that transport or transmit funds they know were derived from criminal activity or are intended to promote criminal activity. Ownership or operation of an unlicensed or unregistered money transmitting business is a general intent crime. Prosecutors need not establish that the defendant knew the business was illegal (i.e., that a licensed was required and no license had been obtained), merely that the defendant knowingly operated a money transmitting business without being licensed or registered.

Violations of this section are punishable by imprisonment of not more than five years, a fine of not more than $250,000 (or $500,000 for organizations), or both. Property involved in a Section 1960 offense may also be forfeited.

6.3.3.1 Virtual Currency Exchanges

Several courts have determined that the scope of Section 1960 includes businesses engaged in the transfer or exchange of virtual currencies.

In United States v. Faiella, the defendants were charged with violating Section 1960 in connection with their operation of an underground market in bitcoin. The court concluded that, for the purposes of Section 1960, bitcoin qualified as both “money” and “funds” because “bitcoin can be easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions.” The court further determined that the defendants were “money transmitters” under Section 1960 in view of FinCEN guidance specifically clarifying “that virtual currency exchanges constitute ‘money transmitters’ under its regulations.”

---

860 United States v. Elfgeeh, 515 F.3d 100, 132-33 (2d Cir. 2008) (Section 1960 “appears still to require proof that the defendant knew that the business was engaged in money-transmitting and also knew that the business had no money-transfer license.”); United States v. Dimitrov, 546 F.3d 409, 413 (7th Cir. 2008) (“[T]he government no longer need prove that a defendant was aware of state licensing requirements or that he knew about the federal registration requirements found at 31 U.S.C. § 5330.”).
864 Id. at 545 (noting that “‘money’ in ordinary parlance means ‘something generally accepted as a medium of exchange, a measure of value, or a means of payment’”) (quoting Merriam-Webster Online, http://www.merriam-webster.com/dictionary/money).
866 Faiella, 39 F. Supp. 3d at 545.
867 Id. at 546.
Two years later, in *United States v. Murgio*, the defendants were charged with various crimes, including violation of Section 1960, in connection with their operation of a virtual currency exchange site, Coin.mx.868 The court ruled that bitcoin fell within the ordinary meaning of “funds” because bitcoin “can be accepted ‘as a payment for goods and services,’ or bought ‘directly from an exchange with [a] bank account.’”869

The *Murgio* court further found that the indictment sufficiently alleged violations of Section 1960 for failure to comply with state and federal regulations governing money transmitters. More specifically, the court concluded that bitcoin, as a medium of exchange, qualified as both “monetary value”870 and “payment instruments”871 under the Florida law requiring money transmitters to obtain a license to operate within the state.872 The court also determined that the indictment sufficiently alleged that the defendant failed to comply with federal money transmitter registration requirements.873

---

869 *Id.* at 707-10 (*citing Faiella*, 39 F. Supp. 3d at 545; *Ulbricht*, 31 F.Supp.3d at 570).
870 “Monetary value” is statutorily defined as “a medium of exchange, whether or not redeemable in currency.” Fla. Stat. § 560.103(21).
871 “Payment instrument” is statutorily defined as “a check, draft, warrant, money order, travelers check, electronic instrument, or other instrument, payment of money, or monetary value whether or not negotiable.” Fla. Stat. § 560.103(29) (emphasis added).
873 *Id.* at 714-15.
Chapter 7

7 Cybercrimes

7.1 Hacking/Theft

Hacking is the act of illegally using a computer to access information stored on another computer system or to spread a computer virus. Hacking is possible because security was not built into the original design of the Internet, an omission due primarily to the first Internet developers’ failure to foresee its scaling to become the hub of global commerce.

Hackers today are more efficient than ever due to the universal acceptance of personal computers and the Internet combined with the dramatic increase in computing speeds. Further, law enforcement has not served as much of a deterrent because hackers have a less than 1% chance of being prosecuted and convicted for their crimes.

Hackers can generally be categorized into three different types. The first is the “black hat” hacker, who acts maliciously and hacks for financial gain, revenge, or political or philosophical motivation. Black hat hackers are typically engaged in criminal activity since they act without the permission of developers or administrators. The most successful blockchain hacks committed by black hat hackers were the DAO and Bitfinex attacks, discussed below.

The second type is the “white hat” hacker, who acts without malice, hacking instead for fun or exploration. White hat hackers use their skills to identify vulnerabilities at the request, or with the permission, of their sponsors or employers. Many companies hold so-called “hack-a-thons,” where groups of hackers compete to find vulnerabilities in software source code or to evade

876 Id.
879 See infra Sections 7.1.2.1 and 7.1.2.4.
880 Ruesink, supra note 878.
881 Id.
security and gain access into supposedly secure areas. The hackers who win these competitions tend to be rewarded financially for their efforts.

Many large companies, including Facebook, Google and Microsoft, offer financial rewards and recognition to hackers for reporting bugs. The companies offer a “Bug Bounty” and the hackers, or “Bug Bounty Hunters,” compete for positions in league tables based on the quantity and severity of the bugs that they discover. Companies have been known to offer significant payouts, with some white hat hackers reportedly earning up to $100,000 a year. The Ethereum Foundation has established its own bug bounty program, with payouts of up to $25,000 for the reporting of a critical bug. In addition to the financial rewards for identifying security issues, bug bounty hunters who achieve high leaderboard placements are well respected in software communities.

Hackers that exploit flaws in cryptocurrency software often stand to make significant financial gains, but white hat hackers have proven many times that hackers are not motivated solely by profit. In December 2014, Blockchain.info, a web wallet provider, released a faulty software update that caused insecure private key generation for a small number of users. Consequently, 250 bitcoins, worth around $90,000 at the time, were stolen by hackers. Blockchain.info offered to reimburse users for these losses from its own funds. Thereafter, a white hat hacker reported successfully tracking the vulnerable user addresses and taking possession of the bitcoins to ensure their safety. The hacker then returned the bitcoins to Blockchain.info.

Following the DAO hack, which is described further below in Part 7.1.2.1, several groups of white hat hackers successfully infiltrated the child DAO that had been created by the DAO attacker and secured 7.2 million of the stolen Ether to prevent its permanent misappropriation by

---

883 See, e.g., id.
885 See, e.g., id.
886 Julie Bort, This Hacker Makes an Extra $100,000 a Year as a ‘Bug Bounty Hunter’, Business Insider (May 1, 2016) http://www.businessinsider.com/hacker-earns-80000-as-bug-bounty-hunter-2016-4.
889 Id.
890 Id.
the attacker. While this Ether was subsequently returned to its rightful owners by virtue of the subsequent hard fork, the white hat hackers ended up with the 7.2 million ETC that were created as a result. Subsequently, these white hat hackers have taken steps to return all of the ETC to the corresponding DAO token holders. However, this can only be done if the DAO token holders claim the ETC. While the hackers have tried to set deadlines in an effort to spur this process along, $4.4 million worth of ETC remained unclaimed as of April 15, 2017. The claims deadline, which was extended multiple times, expired on January 10, 2018.

The third type is the “grey hat” hacker, who acts without malicious intent much like a white hat hacker but does so without the consent of the hacked. Grey hat hackers are typically dissidents who hold some belief, or want to perform some action that white hat hackers condemn. Grey hat hackers do not seek to engage in illegal activity for profit like black hat hackers. Grey hat hackers work independently from corporations and have frequently been convicted of cybercrimes, in contrast to white hat hackers who tend to operate either inside the law, for vigilante causes, or with direction from security companies who have paid them to work as bug bounty hunters.

Grey hat hackers are often the most controversial – Anonymous and Lulzsec are two notorious groups – because they use illegal activities to fight for anti-establishment goals. Typically, their attacks target large companies, as opposed to individuals. For example, in 2012, grey hat hacker Andrew “Weev” Auernheimer was arrested and tried in federal court in the District of New Jersey for publishing details concerning a vulnerability in AT&T’s website that allowed iPad users to review their account data by using a specific AT&T URL containing their iPad’s


895 Ruesink, *supra* note 878.


897 *Id.*

898 Ruesink, *supra* note 878.

unique identifying number.\textsuperscript{900} There was no particular harm attributed to Weev’s actions, yet he was convicted of violating the Computer Fraud and Abuse Act. The conviction was later vacated for technical reasons.\textsuperscript{901}

Defenses to hacking are few and far between because source code almost always has vulnerabilities. It takes a considerable amount of programming skill as well as trial and error to discover such vulnerabilities. When one is discovered, developers patch the source code of the program through an update or fork to eliminate the risk of it being exploited. While blockchain technology is susceptible to some exploitation, the generally accepted view is that a blockchain network cannot be hacked because it is distributed on hundreds, if not thousands, of computers throughout the world.\textsuperscript{902} Thus, blockchain networks are immune from the sort of high-profile data breaches that major companies running traditional server-based businesses have suffered.\textsuperscript{903}

7.1.1 Computer Fraud and Abuse Act of 1986

The Computer Fraud and Abuse Act (CFAA) regulates hacking in the United States.\textsuperscript{904} The CFAA bans trafficking, trespass, unauthorized access, espionage, and damage to computers in interstate or international commerce.\textsuperscript{905} The broad language and interpretation of the act means that it governs most online activity. For example, the CFAA prohibits intentional access of a “protected” computer to gain information without authorization.\textsuperscript{906} Although a “protected” computer was originally defined as only machines belonging to the U.S. government and financial institutions, that definition has been expanded over time to cover any computer affecting interstate commerce or communication.\textsuperscript{907} Due to the interstate nature of Internet communication, this broad definition subjects any person using an ordinary Internet-connected personal computer or mobile device to CFAA jurisdiction.\textsuperscript{908}


\textsuperscript{901} \textit{United States v Auernheimer}, 748 F.3d 525 (3d Cir. 2014).

\textsuperscript{902} Toshendra Kumar Sharma, \textit{Where is Blockchain Hosted & Why It Is Difficult to Hack It?}, Blockchain Council (Feb. 9, 2018), \url{https://www.blockchain-council.org/blockchain/where-is-blockchain-hosted-why-it-is-difficult-to-hack-it/}.

\textsuperscript{903} \textit{Id}.

\textsuperscript{904} 18 U.S.C. § 1030.

\textsuperscript{905} \textit{Id}; \textit{see also} Michael Chertoff, \textit{A Public Policy Perspective of the Dark Web}, 2 J. Cyber Pol’y 26 (Mar. 13, 2017), \url{http://www.tandfonline.com/doi/full/10.1080/23738871.2017.1298643}.

\textsuperscript{906} 18 U.S.C. § 1030(e)(2).

\textsuperscript{907} \textit{Id}.

\textsuperscript{908} Corey Varma, \textit{What is the Computer Fraud and Abuse Act (CFAA)?} (Jan. 3, 2015), \url{http://www.coreyvarma.com/2015/01/what-is-the-computer-fraud-and-abuse-act-cfaa/#protected_computer}. 

COPYRIGHT © 2019, BY BLOCKCHAINS, LLC
In *United States v. Trotter*, the defendant challenged this broad interpretation of “protected computer,” arguing that his former employer’s computer network did not meet the definition. The Eighth Circuit affirmed the conviction, noting the defendant had admitted that the computer was connected to the Internet and used in interstate communication, and finding that such traits fit the plain meaning of the statute. Subsequent rulings have consistently affirmed this interpretation of the CFAA, and the criminal penalty for exceeding authorized access to a protected computer has often been used to prosecute individuals who violate the terms of service of Internet sites. Considering that the terms of service for some websites run up to 30,000 words, 73% of Internet users admit to not reading them, and only 17% claim to understand them, it seems all but a few Internet users are operating on “protected computers.”

While prosecution for violating a website’s terms of service are rare, the CFAA has been used to prosecute individuals who have exploited websites even where the targeted company suffered no actual damages. In *United States v. Swartz*, defendant Aaron Swartz used a Massachusetts Institute of Technology (MIT) computer to access the digital library JSTOR, downloading 4.3 million journal articles over several days. While facilitating the downloading of articles is the sole purpose of JSTOR, and there is no need to purchase them individually where a user has authorized access, the mass-download negatively impacted access to JSTOR’s servers, which is prohibited under their terms of service. While Swartz’s intent was unknown, he had a history of downloading information for the purpose of releasing it to the public for free. Swartz was identified and prosecuted under the CFAA for violating JSTOR’s terms of service, computer fraud, unlawfully obtaining information from a protected computer, and recklessly damaging a

---

909 *United States v. Trotter*, 478 F.3d 918 (8th Cir. 2007).


911 *United States v. Trotter*, supra note 909.


918 JSTOR, *JSTOR Evidence in United States vs. Aaron Swartz* (Jul. 30, 2013), [https://docs.jstor.org/summary.html](https://docs.jstor.org/summary.html).
protected computer. This occurred despite a press release issued by JSTOR after his arrest indicating that it had no interest in being involved in the case. Swartz took his own life shortly before trial. If he had been convicted, however, he would have faced up to 35 years in prison and a fine of up to $1 million. Subsequently, the two federal prosecutors involved in the case were criticized for their overzealous prosecution, underscoring the risk of governmental abuse of the CFAA’s broad scope.

While there have been no instances yet of prosecution under the CFAA for actions performed solely on a blockchain ledger, the CFAA has been applied in the vast majority of recent criminal cases involving computers. The CFAA computer fraud provision has been used for indictments related to virtual currency, including that of Silk Road owner Ross Ulbricht on bitcoin money laundering charges. The Ulbricht indictment did not specifically apply the CFAA to blockchain technology; thus, whether the act applies to the technology remains unclear. The most reasonable view seems to be that interacting with an open, public blockchain should not be considered accessing a computer without authorization. However, given the courts’ expansive reading of CFAA liability, an opposite result would not be entirely unexpected.

While the CFAA adequately addresses computer hacking in the United States, it offers little value to law enforcement when the hackers cannot be identified. Further, the CFAA is not effective outside U.S. borders, where the vast majority of cybercrime attacks launched against U.S. companies and individuals originate.

926 Chertoff, supra note 905.
7.1.2 Cyberattacks on Blockchain Applications

7.1.2.1 The DAO

In April 2016, the first decentralized autonomous organization, referred to as “The DAO,” began a 28-day crowdsale to raise funds.\(^{927}\) While leaderless, The DAO was implemented by the owners of German Internet of Things (IoT) company Slock.it, which wrote the smart contracts for The DAO and open-sourced the code.\(^{928}\) To facilitate investment in The DAO, investors sent Ether to The DAO contract in exchange for DAO tokens representing voting rights. The DAO token sale raised a massive $150 million from more than 11,000 investors, making it the world’s seventh largest crowd-funding project to date.\(^{929}\)

The DAO officially launched in May 2016, with token holders preparing at that time to begin making investment decisions for the Ether placed in The DAO contract. Before that happened, however, three researchers from Smartwallet, Ethereum Foundation and Cornell University released a paper calling for a temporary moratorium on investments because they had found nine potential security vulnerabilities in the code for executing The DAO contracts.\(^{930}\) In early June of 2016, before a decision had been reached on the moratorium issue, an Ethereum developer identified a flaw in The DAO code relating to recursive calls, which was a programming bug that allowed an investor to withdraw twice his or her balance out of the contract.\(^{931}\) The Ethereum community then proposed several fixes, which The DAO members were set to vote upon.\(^{932}\) Prior to the vote, however, a hacker exploited several of the previously highlighted vulnerabilities, including the recursive calls flaw, permitting the hacker to slowly transfer 3.6 million Ether,\(^{933}\) worth about $50 million at the time, into a so-called “child DAO.”

A child DAO is a wallet address that can be accessed only by the hacker. It is formed as a subsection of the parent DAO, so it has the same structure, limitations, and vulnerabilities.\(^{934}\) As

---


\(^{928}\) Id.


\(^{930}\) Dino Mark *et al.*, *A Call for a Temporary Moratorium on The DAO*, Hacking, Distributed (May 27, 2016), [http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/](http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/).


\(^{934}\) Siegel, *supra* note 933.
a result, the child DAO had the same 28-day holding period as The DAO contract, meaning that the hacker could not transfer the Ether to his own wallet until the end of that period. No one was able to put forth a solution that would stop the hacker from continuing to drain Ether into the child DAO. To prevent the hacker from withdrawing the Ether from the child DAO after 28 days, members of the Ethereum mining community were asked to approve a “soft fork” that would incur no rollbacks or rewriting of blocks, and would implement a switch in the basic Ethereum code to prevent any Ether from being moved out of The DAO or its children. Before a vote could occur, however, several members of the Ethereum community identified a bug in the implementation of the soft fork that would open the door to DoS attacks.

Thereafter, a controversial hard fork was proposed that would rewrite the existing DAO rules by creating one new smart contract with a single function: allowing The DAO token holders to withdraw their Ether from The DAO contract. By rewriting the rules on which the Ethereum blockchain executes, the hard fork would effectively travel back in time to create a new chain at the time of the last block before The DAO theft had been mined. This new chain would then exist in the future as if the theft had never occurred.

A group of miners that came to be known as “Ethereum Classic” opposed the hard fork. They argued that code is law, that the original statement of The DAO terms should stand under any circumstance, that occurrences on the blockchain are immutable, and that the decision to modify was leading the Ethereum community down a slippery slope to even more changes in the future. Supporters of the hard fork countered that the hacker should not be allowed to profit from the exploitation because it was ethically wrong, that the slippery slope argument was invalid because people should act rationally and fairly, and that the investors who were victimized by the hack were entitled to the return of their Ether. Amid the discussion over whether to pursue the hard fork, someone claiming to be The DAO hacker promulgated an open letter declaring the

935 Id.
936 Id.
941 Hertig, supra note 938.
action as legal and legitimate, and suggesting legal action against The DAO if the Ethereum community adopted the hard fork.943

Ultimately, the Ether mining community voted heavily in favor of the hard fork, which it concluded was the clear path forward to ensure that The DAO code was no longer susceptible to the security vulnerabilities.944 The hard fork was implemented, and The DAO created a withdrawal smart contract, which allowed investors to request a withdrawal amount from The DAO in order to recoup their stolen Ether.945 After the hard fork, all of the Ether sent to The DAO contract, including the 11.6 million stolen Ether, was placed into the withdrawal account for investors, nearly half of which was reclaimed in a matter of hours.946 In April 2017, 90% of the Ether had been reclaimed, with approximately $4 million of unclaimed Ether remaining in the withdrawal contract.947

Because the Ethereum Classic group refused to accept the hard fork as a solution, its adoption has led to two competing chains and currencies. The original chain, called Ethereum Classic, has substantially less support than the new one, called Ethereum. Also, the market capitalization of the original chain’s cryptocurrency, ETC, is generally about 4-5% of Ether’s.948

7.1.2.2 Coincheck

In January 2018, hackers stole over $500 million from the Coincheck, a Tokyo-based cryptocurrency exchange, making it the largest hack in the history of cryptocurrency.949 After the attack, Coincheck immediately froze deposits and withdrawals for all cryptocurrencies, except bitcoin, to assess the losses. According to Coincheck, the hack only involved NEM coins and the


hackers were able to steal the private key for the hot wallet\footnote{A "hot wallet" is a digital wallet connected to the Internet where cryptocurrency services and exchanges can be paid out or withdrawn instantly.} where the NEM coins were stored.\footnote{Darryn Pollock, \textit{Story of Coincheck: How to Rebound After the ‘Biggest Theft in the History of the World’}, CoinTelegraph, (Apr. 3, 2018), \url{https://cointelegraph.com/news/story-of-coincheck-how-to-rebound-after-the-biggest-theft-in-the-history-of-the-world}.} After the announcement, Coincheck faced severe backlash for storing its NEM in a hot wallet rather than a more secure multisig wallet.\footnote{Id.} Since the breach, Coincheck has identified ten accounts into which the hackers placed the stolen coins, and the company has tagged all of the stolen coins to ensure that they can be tracked if the hackers try to sell them.\footnote{Id.}

Several cryptocurrency traders have filed lawsuits against Coincheck for freezing withdrawals after the hack. Those plaintiffs are demanding that Coincheck return their cryptocurrency, reimburse them for any lost cryptocurrency, and compensate them for the drop in their assets’ value while withdrawals were halted.\footnote{Rebecca Laira, \textit{Major Japanese Brokerage Firm Plans to Rescue Coincheck from its Recent Cyber Attack?}, AMB Crypto (Apr. 3, 2018), \url{https://ambcrypto.com/major-japanese-brokerage-firm-plans-to-rescue-coincheck-from-its-recent-cyber-attack/}.} Using its own capital, Coincheck has begun providing reimbursements to the nearly 260,000 users impacted by the hack.\footnote{Id. (in March 2018, Coincheck paid $435 million as compensation to customers).}

As a result of the hack, the Japanese Financial Services Agency (FSA) has been closely monitoring all Japanese cryptocurrency exchanges and has ordered several exchanges to improve their security measures. As part of this increased oversight, the FSA halted operations for a month on both the FSHO and Bit Station exchanges.\footnote{Yuri Kageyama, \textit{Japan Penalizes Several Cryptocurrency Exchanges after Hack}, Phys.org (Mar. 8, 2018), \url{https://phys.org/news/2018-03-japan-penalizes-cryptocurrency-exchanges-hack.html}.}

\textbf{7.1.2.3 Mt. Gox}

In 2011, the largest virtual currency exchange site at that time, Mt. Gox, was attacked by a hacker with a Hong Kong IP address who compromised an auditor’s account credentials to sell himself $8.75 million of bitcoin using the exchange’s software.\footnote{Alex Hern, \textit{A History of Bitcoin Hack}, The Guardian (Mar. 18, 2014), \url{https://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency}.} The hacker acquired the bitcoin
for virtually nothing by creating an “ask” order at any price, which caused the bitcoin price to plummet from $32 per coin to pennies.\textsuperscript{958}

To prove that it still controlled the exchange site, and to inspire confidence in its customers, Mt. Gox moved 424,242 bitcoin from offline cold storage to a Mt. Gox wallet address.\textsuperscript{959} Later in 2011, Mt. Gox lost an additional 2,609 bitcoin due to a purported transaction malleability issue.\textsuperscript{960} During its operation, Mt. Gox received many complaints for never-arriving withdrawals, likely the result of the slight altering of signatures due to transaction malleability, which had caused withdrawal requests to remain unconfirmed.\textsuperscript{961}

In February 2014, Mt. Gox filed for bankruptcy and took its exchange offline following another claimed loss due to a programming error that caused a customer loss of approximately 800,000 bitcoin, worth $470 million at the time.\textsuperscript{962} While transaction malleability and hackers were initially blamed for the breach and loss of currency,\textsuperscript{963} it was eventually revealed that Mt. Gox had been steadily losing bitcoin for years. Many individuals in the bitcoin community, including Cameron Winklevoss, expressed disbelief that a massive exchange such as Mt. Gox could have a transaction malleability problem and not notice 800,000 bitcoin disappearing over the course of several years.\textsuperscript{964}

Further cementing this concern, Mt. Gox announced in March of 2014 that it had found 200,000 bitcoin, worth $116 million, in an old cold storage wallet that “used an old format.”\textsuperscript{965} Critics, including Winklevoss, began suggesting that the rest of the bitcoin was never actually


\textsuperscript{960} Transaction malleability is a bug permitting someone to change the unique ID of a transaction before it is confirmed on the network, which can, in certain cases, lead to the creation of transactions that are impossible to redeem. \textit{See generally} Ken Shirriff, \textit{Bitcoin Transaction Malleability: Looking at the Bytes}, Ken Shirriff’s Blog, \url{http://www.righto.com/2014/02/bitcoin-transaction-malleability.html}.

\textsuperscript{961} Tabbaa, \textit{supra} note 959.

\textsuperscript{962} \textit{Id}.


hacked but instead had been lost due to inaccessible and poorly maintained cold storage wallets. The litigation that resulted from the Mt. Gox collapse is discussed further in Chapter 17.

7.1.2.4 Bitfinex Bond Issuance

The third largest loss of cryptocurrency was the Bitfinex hack in August 2016, wherein 119,756 bitcoin was stolen from the coin exchange. The theft, worth around $66 million, was a puzzle for some time, with customers uncertain exactly how their money had been lost. Eventually, it was revealed that bitcoin had been taken from users’ segregated wallets, and that Bitfinex’s security provider, BitGo, had signed off on large transactions without full security. In the chaotic wake of the hack, customers struggled to obtain information concerning not just the details of the breach but also the identities of Bitfinex’s owners and where they were located. Before the hack, the exchange handled $407.2 million in monthly trade volume, yet Bitfinex’s origins remain shrouded in mystery.

The details of the vulnerability were somewhat exposed and attributed to the way Bitfinex structured its accounts through multisignature wallets provided by BitGo. Bitfinex users who were trading had a 2-of-3 arrangement whereby two out of three keys were needed to sign transactions. Bitfinex held two of the keys, one of which was stored offline, and BitGo the third. While BitGo’s keys apparently remained safe, Bitfinex’s were compromised, and BitGo was not designed to detect unusual actions, only co-sign and agree to withdrawals. As a result, BitGo approved the requests leading to the drain of nearly one-sixth of Bitfinex’s monthly volume. Since Bitfinex relied on the protection of the multi-signature setup, all user funds were stored in a hot wallet, allowing the withdrawal of a massive number of coins. By exploiting


967 *Id.*


970 Higgins, *supra* note 966.

971 *Id.*

972 *Id.*

973 *Id.*

974 *Id.*

BitGo’s uncapped withdrawal limit, the hacker was ultimately able to steal some $66 million from Bitfinex’s hot wallet.976

While the identity of the hacker who looted Bitfinex remains unknown, some virtual currency traders blame the U.S. Commodity Futures Trading Commission (CFTC) for helping cause the event.977 In June 2016, two months before the attack, the CFTC fined Bitfinex $75,000 for facilitating margin trading without seeking registration as a futures commission merchant.978 The CFTC informed Bitfinex that it had to register unless it could establish that actual delivery to users of bitcoin purchased on the exchange occurred within 28 days of the transaction.979 In response to this CFTC pressure, Bitfinex established a relationship with BitGo and switched its internal cold storage system to the BitGo system whereby BitGo acted essentially as a hot wallet.980 As multi-signature wallets are considered especially safe, exactly how the hackers managed to gain access to the private key stored by Bitfinex remains unknown.

Rather than tying the stolen bitcoin to specific customer accounts, Bitfinex unilaterally opted to “socialize” the loss by spreading it pro rata across all user accounts and reducing their value by 36% each.981 Following the hack, Bitfinex relaunched and replaced the lost account value with Bitfinex “tokens” representing a form of obligation on the part of Bitfinex’s parent company, iFinex, similar to a bond.982 Bitfinex indicated that it planned to redeem all of the tokens once it earned sufficient profits to do so. While many in the virtual currency community were skeptical, Bitfinex announced in April 2017 that it had been able to buy back all of the Bitfinex tokens and

---


977 Higgins, supra note 966.


980 Higgins, supra note 966.


reimburse all of the investors with U.S. dollars due to increased equity conversions and strong operating results.983

7.1.2.5 Youbit/Yapizon

On April 22, 2017, Youbit, at the time known as Yapizon, had four of its hot wallets attacked, resulting in a loss of roughly 3,800 bitcoin, which was 37.08% of its total assets.984 Thereafter, Youbit announced that it would be allocating the loss equally among its customer base and replacing 37% of the bitcoin in each member’s account with a token called “Fei.”985 South Korea’s spy agency, the National Intelligence Service, has claimed that North Korean hackers were behind the attack.986 NIS found that the malware used in hacking the exchanges was created using the same method as the malware used in hacking Sony Pictures and the central bank of Bangladesh in 2014 and 2016, respectively, and that the emails used in the attacks emanated from North Korean Internet addresses.987

A second attack on the Youbit exchange occurred on December 19, 2017, resulting in a loss of “about 17 percent of total assets.”988 Thereafter, Youbit immediately halted deposits and withdrawals. The same day, Youbit announced that it was filing for bankruptcy and would disperse any cryptocurrency in its possession.989

In March 2018, DB Insurance denied Youbit’s insurance claim, alleging that Youbit “violated the advance notice obligation,” which required the company to disclose important information prior to obtaining insurance.990 Youbit had obtained the comprehensive liability insurance policy a mere 20 days before declaring bankruptcy, such that insurance fraud was suspected.991 Despite its controversies, Youbit was able to consummate a sale to Coinbin, another


985 Id.


987 Id.


989 Id.


991 Id.
South Korean exchange, and, on March 21, 2018, transferred to Coinbin all of its assets and its members’ personal information.\textsuperscript{992}

\textbf{7.1.2.6 Bithumb Data Breach}

In June of 2017,\textsuperscript{993} Bithumb, South Korea’s largest bitcoin exchange, was hacked and the company revealed that the thieves stole a database of user information off the personal computer of an employee, via a phishing email, rather than off the company’s internal network.\textsuperscript{994} The stolen information included names, email addresses, and telephone numbers of more than 30,000 users, roughly 3\% of the site’s customers.\textsuperscript{995} The hackers were apparently targeting users’ accounts in an effort to drain their digital wallets. It is reported that through the use of the user’s personal information, the hackers obtained bitcoin worth approximately $7 million.\textsuperscript{996}

The hackers demanded $5.5 million from Bithumb in exchange for deleting the users’ personal information, but Bithumb refused the demand.\textsuperscript{997} As with the other attacks in South Korea, the NIS suspects that North Korea was involved.\textsuperscript{998} In December 2017, South Korea’s Communications Commission imposed fines on Bithumb in the amount of 60 million won (approximately $56,000) for failure to protect its users’ information and mandated that the company establish measures to ensure that no further violations occur.\textsuperscript{999}

\textbf{7.1.3 Cyber-risk Insurance for Losses}

Cyber-risk is the risk that an organization’s information technology systems will be compromised, including by malicious electronic attack, causing disruption of business and

\textsuperscript{992} Id.
\textsuperscript{993} There are reports that the attack occurred in January but was only discovered in June. \textit{North Korea 'Hacked Crypto-Currency Exchange in South'}, BBC (Dec. 16, 2017), http://www.bbc.com/news/world-asia-42378638.


\textsuperscript{995} Id.


\textsuperscript{998} Guerrero-Saade, \textit{supra} note 996.

monetary loss.\textsuperscript{1000} The materialization of this risk typically adversely impacts the organization’s profit margins, brand image, and market capitalization.\textsuperscript{1001} While organizations can invest millions into perimeter security systems such as firewalls, and anti-virus and intrusion detection systems, a new virus or skilled hacker can often compromise even the most secure systems. These attacks result in millions of losses annually.\textsuperscript{1002} Cyber-risk insurance is a viable method for a company to recover from such security breaches. While the potential losses are large, insurers provide cyber-risk coverage at prices that companies are willing to pay because the actual probability of an event, such as the complete breakdown of a network or DDoS attack, is relatively small.

Unlike other categories of insurance, there are no risk standards or formulae that the insurance industry as a whole relies upon to underwrite cyber-risk coverage.\textsuperscript{1003} Most cyber-risk insurance policies cover common reimbursable expenses, including investigation, business losses, privacy, litigation and extortion.\textsuperscript{1004} Covered investigation expenses typically include the necessary forensic investigation to determine what occurred, how to repair the data breach, and how to prevent the breach from recurring, and may also involve the services of a third-party security firm in coordination with law enforcement agencies.\textsuperscript{1005} Covered business losses include monetary losses due to network downtime, business interruption, data loss recovery, and repairing reputation damage, as well as the costs of managing the crisis.\textsuperscript{1006} Covered privacy and notification losses usually include data breach notifications to customers and other affected parties, and credit monitoring for customers whose information was actually or potentially breached.\textsuperscript{1007}

Litigation coverage generally covers litigation expenses related to the breach and release of private information and intellectual property, legal investigations, settlements, and regulatory fines. Extortion coverage can cover cyber extortion through ransomware. Finally, some cyber-insurance policies cover errors and omissions in the company’s performance of services, such as first-party programming errors.\textsuperscript{1008}


\textsuperscript{1001} Arunabha Mukhopadhyay, Cyber-risk Decision Models: To unsure IT or not?, 56 Decision Support Sys. 11 (2013).

\textsuperscript{1002} Id.


\textsuperscript{1005} Id.

\textsuperscript{1006} Id.

\textsuperscript{1007} Id.

When evaluating applications, insurance companies look favorably upon indicators that an organization has effectively assessed its vulnerability to cyberattacks and enabled defenses and controls to protect against the attacks as much as possible. Most insurers consider employee education regarding security awareness – particularly, tactics to prevent phishing and social engineering – as a key component of a protection plan. Insurers also evaluate an organization’s customer data privacy, physical security, and risk assessment.

Specialized insurance policies, such as Bitcoin Insurance Agency, now provide robust cybercrime insurance that protects corporate policyholders and their customers from any acts, errors or omissions of an insured resulting in the theft of bitcoin. Most policies include coverage for errors in technology, processes, and employees that result in theft of bitcoins or their related private keys. In the event of a covered loss, the policy will reimburse the policyholder for the full value of the stolen bitcoin. As cryptocurrency and blockchain technology continue to gain market acceptance, insurance companies are exploring product and coverage options.

A few prominent virtual currency exchange and storage sites maintain some degree of insurance covering hacking and theft. For example, since November 2013, Coinbase has been insured against any losses resulting from a breach of the exchange’s physical or cyber security, or by employee theft. All digital currency that Coinbase holds online is insured. However, since Coinbase holds less than 2% of customer funds online, the remainder of funds held in offline storage appears to be uninsured. Additionally, Coinbase’s policy does not cover losses resulting from a compromise of individual accounts. Thus, customers are not covered where poorly protected login credentials are stolen and used to effectuate withdrawals from the exchange.

Finally, Coinbase, through FDIC insurance, insures fiat in a user’s wallet, up to $250,000. In October of 2018, Gemini Trust Company announced it had obtained insurance coverage for the

---

1009 Lindros & Tittel, supra note 1004.
1012 Id.
1013 Id.
1017 Id.
1018 Id.
digital assets in its custody. The press release indicated that the insurance will be provided through a “global consortium of industry-leading insurers and arranged by Aon.”

7.2 New York Cybersecurity Requirements for Financial Services Companies

In response to several data breaches at financial services companies, as of February 2018, New York requires banks, insurance companies and other financial institutions to prepare and submit an annual Certification of Compliance to the New York Department of Financial Services. The requirements apply to covered entities, defined as those operating, or required to operate, under a license, registration, charter, certificate, permit, accreditation, or similar authorization under New York’s banking, insurance, or financial services law. The purpose of the regulation is to ensure that financial companies maintain cybersecurity programs to protect the integrity, availability, and confidentiality of their information systems. The regulation is very stringent; a covered entity cannot submit an annual certification unless it is in full compliance with the applicable requirements of the regulation at the time of certification.

The design of a cybersecurity program will be based on an entity’s risk assessment. Each entity must implement and maintain a written cybersecurity policy, to be approved by a Senior Officer or board of directors, setting out procedures to protect the entity’s information systems and the non-public personal information stored therein. The policy must address data governance, asset inventory, device management, access controls, identity management, business continuity, disaster recovery planning, systems operations, network security, network monitoring, customer data privacy, physical security, environmental controls, third-party service management, risk

---


1020 Id.


1022 Id.

1023 Id.


1025 Id.
assessment, and incident response.\textsuperscript{1026,1027} Covered entities must review their programs, create a repository to document enterprise-level cybersecurity to ensure they cover the identified areas, and maintain supporting program documentation.\textsuperscript{1028}

New York’s regulation, which is the first of its kind, may well be adopted as a model framework for cybersecurity across the country and become a standard by which negligence is measured for non-compliance.\textsuperscript{1029} This could be either a positive or a negative for the covered entities. It may protect companies from securities fraud or shareholder derivative lawsuits following data breaches, as shareholders have filed such lawsuits after data breaches alleging that ineffective or negligent corporate board oversight contributed to the data breach and resultant declines in shareholder value. To the extent that an entity complied with New York’s requirements, the directors would have a strong defense against such negligence claims. On the other hand, where a company failed to comply with the regulations, prospective plaintiffs could use them as a roadmap for establishing liability.\textsuperscript{1030}

Because the virtual currency companies such as Circle, Ripple, Square, Gemini and Coinbase have all been awarded BitLicenses by the New York Department of Financial Services, they all will be subject to cybersecurity regulations.\textsuperscript{1031,1032}

\begin{flushleft}
\textsuperscript{1027} Quach, \textit{supra} note 1024.
\textsuperscript{1028} EY, \textit{supra} note 1021.
\textsuperscript{1030} \textit{Id.}
\end{flushleft}
Chapter 8
Securities Regulations and Virtual Currency Offerings

8.1 Initial Coin Offerings

An initial coin offering, commonly referred to as an “ICO,” is a fundraising mechanism whereby start-up companies offer investors units of digital assets referred to as “tokens” in exchange for an established cryptocurrency, typically Ether. As regulators and legislators have been slow to address ICOs, these offerings are currently unregulated crowdsales that provide substantial sources of capital for numerous start-ups.

Since January 2017, it is estimated that ICOs have raised over $20 billion. The ICO market significantly slowed in the last three quarters of 2018 and token prices plummeted. According to an Ernst & Young report, of the 141 largest ICOs in 2017, 86% are trading below their list price, while 30% have lost substantially all of their value. The most common factors contributing to the decline in token prices and ICO participation are increased regulatory oversight surrounding ICOs, the lack of meaningful progress towards projects promised by the ICOs, and the continued price decline of the cryptocurrencies utilized to purchase ICO tokens, including bitcoin and Ether.

The tokens sold in an ICO are not equivalent to stocks insofar as they do not provide tokenholders with any ownership interest in the token issuer. Instead, tokens generally have three functions. First, they have their own utility by providing access to certain services, such as cloud storage space, voting rights in an organization, programming power, and more. Second, they are often traded in secondary markets created by exchanges. Many of these exchanges are not properly registered with the relevant regulatory authorities such that many countries,

---


1035 Id., Companies that have made meaningful progress toward working products only increased by 13% in 2018, and 71% of companies have no offering in the market at all.


including the United States, are now cracking down on unregistered exchanges.\footnote{Mike Orcutt, \textit{The Next Generation of ICOs Will Actually Have to Follow the Rules}, Technology Review (Mar. 22, 2018), \url{https://www.technologyreview.com/s/610513/the-next-generation-of-icos-will-actually-have-to-follow-the-rules/}.} Third, if the project that is the subject of the ICO ultimately generates profits, then tokenholders will receive a return on their investments. Notably, this return is generally not guaranteed as to timing or amount.\footnote{Oscar Williams-Grut, \textit{No Wonder Investors Are Rushing into Cryptocurrencies – Average ICO Returns Are 1,320\%}, Bus. Insider (Oct. 18, 2017), \url{http://www.businessinsider.com/ico-mangrove-capital-average-returns-crypto-icos-2017-10}.}

Anyone with Internet access can create an ICO in just a few steps. First, during the initial development phase, a company proposes a project idea to potential backers and releases a whitepaper describing the project. Second, the company provides a window during which anyone can purchase the company’s proprietary tokens in exchange for Ether or bitcoin. Third, during or after the ICO, the company releases the proprietary tokens to investors.

Despite ICOs’ rise in popularity, there is still some security risk due to lack of regulation. Estimates show that up to 10\% of the proceeds of ICOs in 2017 may have been misappropriated due to cybercrimes, such as exploits, hacks, phishing, and Ponzi schemes.\footnote{Chainalysis Blog, \textit{The Rise of Cybercrime on Ethereum} (Aug. 7, 2017), \url{https://blog.chainalysis.com/the-rise-of-cybercrime-on-ethereum/}.} For example, in August 2017, the company behind popular social messaging application Kik launched a high-profile ICO that raised $97.5 million.\footnote{Jon Russell, \textit{Kik Raises Nearly $100M in Highest Profile ICO to Date}, TechCrunch (Sept. 26, 2017), \url{https://techcrunch.com/2017/09/26/kik-ico-100-million/}.} Forty minutes before the ICO’s official launch, a URL for the ICO with a fake wallet address was distributed on social media. Before anyone realized that it was not the real Kik wallet address for the ICO, the malicious wallet address acquired 70.9 Ether, valued at approximately $21,656.

The U.S. Securities and Exchange Commission (SEC) did not issue any guidance on ICOs until August 2017, when it warned potential investors about scammers using ICOs for phishing and “pump and dump” schemes. The SEC advised potential ICO investors to always research a company before buying tokens, to be wary of non-reporting companies that may not disclose accurate accounting information, and to be especially cautious of a company claiming its ICO is “SEC-compliant” without explaining how, or a company that purports to raise capital through an ICO or to take on ICO-related business described in vague or nonsensical terms.\footnote{U.S. SEC, \textit{Investor Alert: Public Companies Making ICO-Related Claims} (Aug. 28, 2017), \url{https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-alert-public-companies-making-ico-related}.} On March 7, 2018, the SEC issued a statement warning the public that many online cryptocurrency platforms provide a mechanism for trading assets that meet the definition of a
“security” under federal securities laws but are not properly registered with the SEC. The statement provides investors with a host of questions to ask before deciding to trade digital assets on an online trading platform and a list of resources where they can find additional information. Lastly, the statement warns exchanges and other market participants that employ new technologies to consult legal counsel or contact SEC staff before offering products or services.

In November 2018, the SEC issued another public statement emphasizing that market participants are expected to adhere to the federal securities law framework, “regardless of whether the securities are issued in certificated form or using new technologies, such as blockchain.” The statement stressed the enforcement actions taken in 2018 against cryptocurrency and exchange companies. The issues in these actions fell into three categories: “(1) initial offers and sales of digital asset securities (including those issued in initial coin offerings (“ICOs”)); (2) investment vehicles investing in digital asset securities and those who advise others about investing in these securities; and (3) secondary market trading of digital asset securities.”

8.2 Investor Protection Issues

Prior to 2018, there was minimal guidance on the regulatory scheme of ICOs and exchanges, leading some companies to raise substantial funds by providing potential investors with merely brief descriptions of their projects. The SEC recently stepped up its enforcement actions to protect ICO investors.

8.2.1 Offer and Sales of Digital Asset Securities

The SEC continues to develop a regulatory framework for the offer and sales of digital assets and securities to protect investors. Recent enforcement actions make clear that certain digital assets qualify as “securities” and must thus be registered with the SEC to provide investors with proper disclosures as required by federal securities laws.

8.2.2 Investment Vehicles Investing in Digital Asset Securities

The SEC has applied the Investment Company Act of 1940 to digital assets, stating that the Act’s framework “applies to a pooled investment vehicle, and its service providers, even when the securities in which it invests are digital asset securities.” Therefore, investment vehicles that hold digital assets and securities and those who advise others about investing in digital asset

---


1047 Id.

1048 Id.


1050 Id.

1051 Id.


1053 U.S. SEC, supra note 1049.
securities, including managers of investment vehicles, must assess their registration, regulatory and fiduciary obligations under the Investment Company Act and the Investment Advisers Act of 1940.1054

8.2.3 Trading of Digital Asset Securities

Finally, the SEC is monitoring secondary market trading of digital assets to ensure that those who meet the statutory requirements of a national securities exchange or broker or dealer actually register as such, unless an exemption applies.1055

8.3 Securities Law Issues

A company seeking to raise money in the United States is subject to the Securities Act of 1933 (the “Securities Act”),1056 which requires the registration of all sales of security financial instruments, unless an exemption is available. Where no exemption exists, private companies must comply with the initial public offering (IPO) requirements1057 prescribed by the SEC. In an IPO, a company sells previously unissued securities and receives all proceeds in the form of additional capital, which is considered its primary offering.1058 A securities sale in which the owners’ shares are sold is considered a secondary offering.1059

The reasons why a company would want to be publicly listed include raising capital, using stock as currency to acquire other companies, attracting talented employees, diversifying investor holdings, providing liquidity for shareholders, and enhancing reputation. In a traditional IPO, a company employs underwriters and files a registration statement with the SEC in which it makes specific disclosures (outlined below) about its business and finances, conducts a presentation generally targeting institutional investors, and prices the offering based on a declaration from the SEC that the registration statement is effective. The company then lists securities on an exchange to provide a trading market.

If the token offered in an ICO is classified as a security, an issue discussed at length below, and the issuer cannot qualify for any exemption from registration, then the issuer must comply with all SEC rules for an IPO. The basic disclosure requirements for registration of an IPO include:

1) A description of the company’s business, properties, and competition;
2) A description of the risks of investing in the company;
3) A discussion and analysis of the company’s financial results and financial condition as seen through the eyes of management;

1055 U.S. SEC, supra note 1049.
1058 Id.
1059 Id.
4) The identity of the company’s officers and directors and their compensation;
5) A description of material transactions between the company and its officers, directors, and significant shareholders;
6) A description of material legal proceedings involving the company and its officers and directors;
7) A description of the company’s material contracts;
8) A description of the securities being offered;
9) The plan for distributing the securities; and
10) The intended use of the proceeds of the offering.1060

While an IPO offers the opportunity to raise capital quickly and reach a large number of investors, one major disadvantage is the time and expense of undergoing the process. It is common for an IPO to take between six and nine months, assuming that it is coordinated and managed properly.1061 The financial audit, preparation and review of the registration statement, review by the SEC, and final review by the stock exchange are all lengthy processes; yet, they could be even lengthier for a blockchain start-up, considering the reviewers’ potential incomprehension of the technology. Other important aspects of the company’s business, such as project development, may suffer due to management being overly focused on the IPO. Filing for a public offering also involves substantial direct costs, including those for attorneys, auditors, and underwriters, and filing fees. As the IPO launch date approaches, the company will need to spend more money on marketing costs to ensure that the investing public and institutional investors are aware of the upcoming offering.

Even after an IPO succeeds, the company must comply with strict disclosure requirements for financial statements and accounting and tax matters – all of which require more resources to hire a team of lawyers and auditors to ensure compliance with relevant regulations. Once a company goes public, moreover, shareholders gain a significant ownership stake in it, which opens the door to the possibility of a hostile takeover by a larger company. In an attempt to avert such a takeover, managers of the public company may make poor business decisions, sacrificing long-term growth to satisfy shareholders with short-term profits.

Considering that IPO requirements are burdensome, time-consuming, and costly, even legitimate ICO issuers may prefer not to go public. An ICO is arguably easier and cheaper to organize than an IPO; and where a token issuer would prefer to host an ICO, the issuer must ensure that the token does not constitute a security, triggering the requirements for an IPO.

1060 U.S. SEC, Information for Small Businesses
1061 The Motley Fool, Advantages and Disadvantages of Going Public Using an IPO,
8.3.1 The Howey Test

The SEC has taken the position that “ICOs, based on specific facts, may be securities offerings, and fall under the SEC’s jurisdiction of enforcing federal securities laws.” However, the SEC acknowledges that there are instances where digital assets are not necessarily securities. Thus, when determining whether an ICO qualifies as a security, companies must assess not only the underlying rights associated with the digital asset during the ICO but also the manner of sale and reasonable expectations of purchasers.

An ICO issuer who wants to raise capital without registration must structure the token so that it does not qualify as a security. Section 2(a)(1) of the Securities Act defines a security as:

any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, investment contract or, in general, any interest or instrument commonly known as a ‘security,’ or any certificate of interest of participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.

The same definition can be found in §3(a)(10) of the Securities Exchange Act of 1934. Whether a particular ICO token meets the ‘security’ definition is governed by the test set forth by the U.S. Supreme Court in SEC v. Howey.

In Howey, the U.S. Supreme Court held that the offer of a land sales and service contract constituted an “investment contract” for purposes of the Securities Act. In reaching this conclusion, the Court promulgated a four-prong test that has been followed by the SEC and courts for more than 70 years. Specifically, the Court held that an investment is a security where there is “(i) an investment of money (ii) in a common enterprise (iii) with an expectation of profits (iv) solely from the efforts of others, regardless of whether the shares in the enterprise are evidenced by formal certificates or by nominal interest in physical assets of the enterprise.” All four of these factors must be satisfied for an investment product, such as an ICO token, to be considered a security.

---

1068 Howey, 328 U.S. at 298-99.
8.3.1.1 Investment of Money

Courts have broadly defined the investment of money to include capital, assets, cash, goods, services, or a promissory note. In SEC v. Shavers, a federal court held that bitcoin satisfies the “investment of money” prong of the Howey test because it has a measure of value, can be used as a form of payment, and is used as a method of exchange. The court further stated that, while bitcoin lacks the status of legal tender, legal tender status is not a prerequisite for establishing that investments constitute an investment contract.

However, a federal court in SEC v. Blockvest, LLC denied the SEC’s request for a preliminary injunction, citing that “the subjective intent of the purchaser may have some bearing on the issue of whether they entered into investment contracts.” The SEC argued that Blockvest’s website and whitepaper presented an offer of an unregistered security in violation of Section 5 of the Securities Act. The Court noted that the SEC’s argument presumed, without evidentiary support, that the 32 test investors who purchased tokens had reviewed the Blockvest website, the whitepaper and media posts when they clicked the “buy now” button on Blockvest’s website. However, the SEC and the Defendants provided very different facts as to what the 32 test investors relied on – in terms of promotional materials, information, economic inducements or oral representations at the seminars – before purchasing the test BLV tokens. Therefore, because there were disputed issues of fact, the Court could not make a determination whether the test BLV tokens were “securities” under the first prong of Howey, because it was unclear what materials the investors relied upon when deciding to purchase the BLV.

8.3.1.2 Common Enterprise

Federal courts have developed three approaches for determining when a common enterprise exists: (i) horizontal; (ii) narrow vertical and (iii) broad vertical. The horizontal

---

1072 Id. at 5.
1073 Id. at 16.
1075 Id. at 6-9.
1076 Id.
1077 Id.
1078 Id. at 9.
approach is applied by the First, Second, Third, Fourth, Sixth, and Seventh Circuits. Under the horizontal analysis, a common enterprise is found where multiple investors pool funds and each investor’s profits are correlated with those of the other investors. The sharing of funds is key to satisfy the common enterprise horizontal analysis. Thus, where there is no pooling of funds or sharing of profits, a common enterprise will not be found.

In *Hirk v. Agri-Research Council, Inc.*, for example, the court rejected the plaintiff’s claim that an agreement entered into with the defendants constituted an “investment contract” under the Securities Act, ruling that there was no “common enterprise.” Specifically, the court held that the defendant’s overlapping investment services and the similarity of concomitant transactions in various discretionary trading accounts did not transform the plaintiff’s single account into a joint account with other investors. On appeal, the Seventh Circuit rejected the plaintiff’s argument that there was a common enterprise because different investors’ funds had been comingle, finding instead that each investor’s profits were based on transactions specific to that investor.

Under the horizontal analysis, in the ICO context, it may be possible to show a common enterprise based on the fact that tokens are widely considered an investment with an expected return that will be the same for all investors. This commonality of return exists because the value of a token and entitlement to profits does not differ between investors.

The narrow vertical analysis, by contrast, finds a common enterprise if there is some correlation between the fortunes of the investor and promoter. The Ninth Circuit is the only court that follows the narrow vertical analysis. In *SEC v. Eurobond Exchange Ltd.*, the district court granted summary judgment to the SEC on a disgorgement claim, rejecting the defendant’s argument that there was no common enterprise since investors did not share profits with the corporation.

The Ninth Circuit acknowledged that there was some truth to the defendant’s contention that compensation was paid up front rather than from profits but cited another contract clause suggesting that the corporation had shared profits with investors under certain circumstances. The court of appeals further noted that the investor’s success was correlated with the corporation’s

---

1079 *SEC v. SG Ltd.*, 265 F.3d 42 (1st Cir. 2001).
1080 *Revak v. Realty Corp.*, 18 F.3d 81, 87 (2d Cir. 1994).
1084 *Hirk v. Agri-Research Council, Inc.*, 561 F.2d 96 (7th Cir. 1977).
1086 *Hirk*, 561 F.2d at 101.
1087 *Id.* at 104.
1088 *Id.* at 101.
1089 *SEC v. Eurobond Exchange Ltd.*, 13 F.3d 1334 (9th Cir. 1994).
1090 *Id.* at 1339.
insofar as they shared the risk of loss from default on the foreign bonds sold by the corporation.\textsuperscript{1091}
As the Ninth Circuit summarized, where an investor’s avoidance of loss depends on the promoter’s “sound management and continued solvency,” a common enterprise exists.\textsuperscript{1092}

Finally, under the broad vertical analysis, “a common enterprise is one in which the fortunes of the investor are interwoven with and dependent upon the efforts and success of those seeking the investment of third parties.”\textsuperscript{1093} In this analysis, “the critical factor is not the similitude or coincidence of investor input, but rather the uniformity of impact of the promoter’s efforts.”\textsuperscript{1094} Basically, any time an investor’s success depends upon a promoter’s expertise, the broad vertical analysis will likely support a finding of a common enterprise between them. The Fifth and Eleventh Circuits\textsuperscript{1095} both follow this approach.

In \textit{SEC v. Continental Commodities Corp.},\textsuperscript{1096} for example, the Fifth Circuit reversed a district court’s order denying a preliminary injunction sought by the SEC. The district court had based its denial, in part, on the conclusion that the defendant’s trading in discretionary commodities accounts did not amount to an investment contract because different types of investments were made for different investors. The Fifth Circuit, however, rejected the district court’s holding that “congruity of investment” was required for there to be a common enterprise, ruling instead that “the critical inquiry is confined to whether the fortuity of the investments collectively is essentially dependent upon promoter expertise.”\textsuperscript{1097}

The broad vertical analysis is generally the easiest to satisfy because it focuses on whether the investor relied upon the promoter’s expertise, and the promoter often is more knowledgeable than the investor. Similarly, in cases where the investor stands to gain profit in the same manner as the investor, irrespective of expertise, the narrow vertical test is readily satisfied. The most widely used test, the horizontal analysis, is the hardest to meet. Unlike both vertical tests, the horizontal analysis requires there to be a common financial interest among the investors, which often is not the case, meaning there are many circumstances where allegations sufficient for the former are insufficient for the latter.\textsuperscript{1098}

\textsuperscript{1091} \textit{Id.} at 1340.

\textsuperscript{1092} \textit{Id.} (quoting \textit{United States v. Carman}, 577 F.2d 556, 563 (9th Cir. 1978).

\textsuperscript{1093} \textit{SEC v. Koscot Interplanetary, Inc.} 497 F.2d 473, 478 (5th Cir. 1974).

\textsuperscript{1094} \textit{Id.} at 478.

\textsuperscript{1095} See \textit{id.; SEC v. ETS Payphones, Inc.}, 300 F.3d 1281 (11th Cir. 2002).

\textsuperscript{1096} \textit{SEC v. Continental Commodities Corp.}, 497 F.2d 516 (5th Cir. 1974).

\textsuperscript{1097} \textit{Id.} at 522.

\textsuperscript{1098} See \textit{Deckebach v. La Vida Charters, Inc.}, 867 F.2d 278 (6th Cir. 1989); \textit{Salcer v. Merrill Lynch, Pierce, Fenner & Smith, Inc.}, 682 F.2d 459 (3d Cir. 1982).
8.3.1.3 Expectation of Profits

In *SEC v. Edwards*, 1099 the Supreme Court held that expected profits may include dividends, other periodic payments, or the increased value of the investment (whether variable or fixed-term). Since the “expectation of profits” element of the *Howey* test is so broadly defined, this prong would very likely be satisfied in most ICOs. Indeed, ICO tokens are purchased with the expectation that they will, at some point, rise in value and provide some return on investment. If a showing can be made that a certain ICO has been developed for non-profit, charitable means, then the question of whether it could be considered a security would be moot because there would be no return on investment. Where the token has a completely independent utility that provides significant rights to the token holder aside from investment, such as for use as cloud storage or as programming power, this prong can be rebutted.

8.3.1.4 Solely from the Efforts of Others

The final prong of the *Howey* test requires showing that the success of the investment turns solely on the efforts of others. 1100 An issuer might avoid having its ICO token classified as a security by stipulating that the purchase of tokens affords the holders voting rights to assist with development of the issuer’s project. Whether these voting rights are sufficient for a court to find that the success of the investment “turns solely on the effort of others” depends on several factors, including whether the voting rights provide an ability to significantly participate in decisions affecting the success of the business, whether the ICO targets the pool of tokenholders for their expertise in order to seek a meaningful contribution to the project, and whether the tokenholder actually participates in the voting process. 1101

There are two circumstances where an ICO may potentially avoid classifying its token as a security. The first is where the ICO is for a project using open source software on a public blockchain, and the ICO directs the sale of tokens to a defined group of individuals who can meaningfully work together on the project and are not widely dispersed. Such an arrangement would have a strong argument under this final prong of the *Howey* test. Per the SEC report discussed below, however, it is critical both that the defined group of individuals be chosen for their expertise and that token holders expect to use this expertise to assist in development of the project as a working unit. This is necessarily a fact-dependent determination, so there are no guarantees as to how the SEC or a court will rule.

The second circumstance occurs where the ICO issues tokens with independent utility. If the token has some substantial use besides investment, the “expectation of profits” prong of the *Howey* test may be irrelevant insofar as the primary reason for purchasing tokens is not to make money. The blockchain company Circle, for example, announced on October 5, 2017, that it was launching an open source project providing technology to enable a global network of peer-to-

---


1101 *Klaers v. St. Peter*, 942 F.2d 535 (8th Cir. 1991) (finding that non-managing partners could not have expected profits solely from the defendant’s efforts, because those partners collectively controlled 80% of voting power on any items affecting the partnership, giving them the ability to substantially affect the business).
Circle intends to launch an ICO of utility tokens that can be used to facilitate transfers and pay for services on this network. The open source implementation is built on the Ethereum blockchain but will run on other blockchains, and the company plans to form a non-profit foundation called “Centre Foundation” to manage the protocol. That Circle is issuing tokens with an independent use and running the project through a non-profit foundation means its tokens will likely be considered “non-security.”

Further, someone who purchases a token with independent utility after the ICO has occurred does not expect future return from “the efforts of others” because most of the managerial work on the project was already completed during the development stage, before the token was issued. The issuer’s managerial efforts are the primary determinants of a utility token’s price during the pre-launch phase because that utility is not yet functional. For this reason, the creators of the SAFT project, discussed below, take the position that, while utility tokens are not necessarily securities, they should be treated as such during the pre-launch, non-functional stage, before they become independently useful.\footnote{Juan Batiz-Benet \textit{et al.}, \textit{The SAFT Project: Toward a Compliant Token Sale Framework}, Protocol Labs (Oct. 2, 2017), \url{https://saftproject.com/static/SAFT-Project-Whitepaper.pdf}.}

\subsection{SEC Report on The DAO}

The DAO was the first Decentralized Autonomous Organization to attempt to provide an open source, decentralized business model for organizing commercial and non-profit enterprises on the Ethereum blockchain.\footnote{Bryan Smith, \textit{The Story of the DAO, and How It Shaped Ethereum}, Coin Insider (May 23, 2018), \url{https://www.coininsider.com/what-happened-to-the-dao/}.} The DAO sold $150 million worth of tokens to investors in exchange for the opportunity to vote on which blockchain projects the funds would be invested in and to share in the profits from those projects. The plan was for proposals to be submitted in the form of smart contracts supported by the Ethereum blockchain and for votes to be administered by the code of the DAO. Before the proposal stage was reached, however, a hacker exploited a security flaw in The DAO contract to misappropriate $50 million worth of Ether, forcing termination of the organization.\footnote{See \textit{generally} Chapter 7, Section 7.1.2.1.}

On July 25, 2017, the SEC released a report on its investigation of The DAO pursuant to §21(a) of the Securities Exchange Act of 1934 (the “SEC Report”).\footnote{SEC, \textit{Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO}, Release No. 81207 (Jul. 25, 2017), \url{https://www.sec.gov/litigation/investreport/34-81207.pdf}.} The SEC Report examined whether federal securities laws applied to issuance of The DAO tokens, including the threshold inquiry as to whether they were securities, answering both questions in the affirmative. In reaching these conclusions, the SEC stressed that the \textit{Howey} test “permits the fulfillment of the statutory purpose of compelling full and fair disclosure relative to the issuance of ‘the many types of

\begin{itemize}
\item peer payments.\footnote{Laura Shin, \textit{Blockchain Startup Circle to Launch Open Source Project to Send Money Like Email and Text}, Forbes (Oct. 5, 2017), \url{https://www.forbes.com/sites/laurashin/2017/10/05/blockchain-startup-circle-to-launch-open-source-project-to-send-money-like-email-and-text/#1276554b1593}.}
\item 8.3.2 SEC Report on The DAO
\item 8.3.3 Summary
\item 8.4 Conclusion
\item 8.5 Appendix
\end{itemize}
instruments that in our commercial world fall within the ordinary concept of a security,”1107 and that “emphasis should be on [the] economic realities underlying a transaction, and not on the name appended thereto.”1108

Applying the first prong of the Howey test, the SEC Report determined that investors made an investment of money by exchanging Ether for The DAO tokens,1109 and that they did so with a reasonable expectation of profits, as evidenced by various promotional materials touting The DAO’s status as a for-profit entity.1110 In terms of the second prong, the SEC Report determined that these profits were to be derived solely from the efforts of others even after The DAO’s launch. Investors reasonably expected to profit from the future managerial and entrepreneurial efforts of Slock.it, its co-founders, and a group of persons called the “Curators,” who had been chosen by Slock.it specifically for their expertise.1111

In finding that there was a common enterprise, the SEC framed its inquiry primarily in terms of the broad vertical analysis: i.e., “whether the efforts made by those other than the investor are the undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise,”1112 As the SEC Report noted, most important managerial functions were reserved for the Curators, effectively eliminating tokenholders’ control over the organization.1113 The SEC characterized tokenholders’ ability to vote as largely perfunctory and noted that they were too widely dispersed to effect meaningful control or change.1114

The SEC Report hinged on the fact that investors expected to rely extensively on the efforts of The DAO’s Curators rather than having a meaningful role through voting. Also underlying its conclusions was the implicit point that The DAO tokens had no real non-investment utility. ICO issuers hoping to issue tokens that do not qualify as securities under the Howey test can take solace in the fact that the SEC did not categorically rule that all ICOs require registration and compliance with the IPO rules. The door is still open for non-registered ICOs, particularly those that offer tokens with independent utility, which are now frequently characterized as “non-security tokens.”1115

1107 SEC v. Howey, 328 U.S. at 299.
1109 SEC Report (citing Uselton v. Comm. Lovelace Motor Freight, Inc. 940 F.2d 564, 574 (10th Cir. 1991) (“In spite of Howey’s reference to an ‘investment of money,’ it is well established that cash is not the only form of contribution or investment that will create an investment contract.”); see also Mem. Op., SEC v. Shaver, supra note 1071.
1110 Id. at 11-12 (citing Edwards, 540 U.S. at 394).
1112 Id. at 13 (citing SEC v. Glenn W. Turner Enters., Inc., 474 F.2d 476, 482 (9th Cir. 1973)).
1114 Id. at 14.
8.3.3 Crowdfunding Exemption for ICOs Below $1,000,000

While larger ICOs must steer clear of the elements of a security identified in the Howey test, smaller ICOs can take advantage of the crowdfunding exemption to the IPO registration requirements. Crowdfunding is the method of raising capital for a project or venture by raising small amounts of money from a large number of people, usually through the Internet.\(^{1116}\)

In 2012, the Jumpstart Our Business Startup (JOBS) Act\(^{1117}\) created an exemption from registration for crowdfunding transactions.\(^{1118}\) The exemption was added to the Securities Act and in 2015 the SEC adopted Regulation Crowdfunding, which has been available for use since May 16, 2016.\(^{1119}\) “Small amounts of money” as interpreted by the exemption, means less than $1 million total. Additionally, issuers must cap individual contributions based on net worth or annual income. Individual investors are annually limited in the amounts they are allowed to invest in all Regulation Crowdfunding offerings. If an investor’s net worth or annual income is less than $107,000, the investor’s limit is the greater of $2,200 or 5% of the lesser of the investor’s annual income or net worth. Consequently, using the crowdfunding exemption means foregoing any significant contribution from most individuals who invest in the project.

While an exempt issuer needs not comply with the complete IPO requirements of the Securities Act, any issuer conducting a Regulation Crowdfunding offering must provide a disclosure statement setting forth certain information, including:\(^{1120}\)

1) Information about officers, directors, and owners of 20% or more of the issuer;
2) A description of the issuer’s business and the use of proceeds from the offering;
3) The price to the public of the securities or the method for determining the price;
4) The target offering amount and the deadline for reaching that amount;
5) Whether the issuer will accept investments in excess of the target offering amount;
6) Certain related-party transactions; and
7) A discussion of the issuer’s financial condition and financial statements.\(^{1121}\)


\(^{1117}\) 112 P.L. 106.


\(^{1120}\) Id.

\(^{1121}\) Id.
8.3.4 Recent SEC Enforcement Actions and Class Actions for Unregistered ICOs

There has been a significant uptick in private class actions and SEC enforcement actions filed against cryptocurrency companies that have failed to register their ICOs in accordance with securities laws.

For example, in 2017, four class action lawsuits, which were later consolidated, were filed against Tezos Stiftung (Tezos) and various project participants, alleging that the defendants had conducted an unregistered ICO between July 1 and 14, 2017, raising $232 million, in violation of the Securities Acts of 1933 and of 1934. The defendants moved to dismiss the consolidated action on several grounds, including the improper extraterritorial application of the Securities Exchange Act of 1934, since Tezos claimed that all of the relevant transactions had taken place in the Channel Islands. In its order denying the motion to dismiss against the primary defendants, the court assessed whether the transaction was domestic or foreign, which depended on where a transfer of title or instance of “irrevocable liability” to purchase or pay for a security had occurred. The court highlighted several factors that, taken together, supported an inference that the actual situs of the transaction was in the United States. These factors included that the token sale website was hosted in Arizona, the website was run primarily by a California resident, the token sale marketing almost exclusively targeted United States residents, and the purchaser contributions were validated by a network of global nodes clustered more densely in the United States than in any other country. The case is currently pending in the United States District Court, Northern District of California.

The SEC has also filed numerous enforcement actions against companies that have conducted unregistered ICOs. For example, in late 2017, two blockchain companies – CarrierEQ, Inc. (Airfox) and Paragon Coin, Inc. (Paragon) – conducted unregistered ICOs after the SEC warned that digital assets may be considered securities offerings in its DAO Report of Investigation. Through its ICO, Airfox raised approximately $15 million to finance its development of a mobile application “that would allow users in emerging markets to earn tokens and exchange them for data by interacting with advertisements.” Paragon raised approximately

---


1123 *Id.*


1126 *Id.*

1127 *Id.*


1129 See infra Section 8.3.2.

1130 *Id.*
$12 million through its ICO to develop and implement its business plan of adding blockchain technology to the cannabis industry.\textsuperscript{1131} Without any notice that an enforcement action had commenced against the companies, the SEC announced on November 16, 2018 that it had accepted settlements from both Airfox and Paragon.\textsuperscript{1132} The consent orders imposed $250,000 worth of penalties and included undertakings to compensate harmed investors.\textsuperscript{1133} The companies were also ordered to register their tokens as securities pursuant to the Securities Exchange Act of 1934 and to file periodic reports to the Commission for at least one year.\textsuperscript{1134} This is the first time the SEC penalized issuers of ICOs that had not committed fraud by violating the registration requirements of U.S. securities laws.

In January 2018, the SEC obtained a court order halting AriseBank’s ongoing ICO that targeted retail investors to invest in what was claimed to be the world’s first “decentralized bank.”\textsuperscript{1135} Among other allegations, the SEC’s injunction application stated that AriseBank had failed to register its tokens as securities, and had fraudulently claimed that the ‘bank’ was FDIC-insured.\textsuperscript{1136} On December 11, 2018, the SEC and AriseBank agreed to settle the underlying case. The settlement requires the company and its executives to pay approximately $2.7 million in disgorgement of ill-gotten gains, penalties, and interest.\textsuperscript{1137} Additionally, the company’s CEO, Jared Rice, Sr., and COO, Stanley Ford, are prohibited indefinitely from serving as officers or directors of public companies or participating in further offerings of digital securities.\textsuperscript{1138}

In April 2018, the SEC filed a complaint in the Southern District of New York against Centra Tech., Inc. and its co-founders for violating anti-fraud and registration provisions of the federal securities laws.\textsuperscript{1139} The executives claimed that funds raised through the ICO would help build a suite of financial products, including the offering of a debit card backed by Visa and Mastercard that would allow users to instantly convert “hard-to-spend” cryptocurrencies into fiat

\textsuperscript{1131} Id.

\textsuperscript{1132} In January 2018, a class action lawsuit was filed against Paragon for failing to register the offer and sale of a security under the Securities Act of 1933.\textsuperscript{1132} Paragon filed a motion to dismiss the complaint in October 2018. The hearing is set for March 2019. Motion to Dismiss, Astley Davy v. Paragon Coin, Inc. et al., No. 3-18-cv-00671 (N.D. Cal. Oct. 4, 2018).

\textsuperscript{1133} Id.

\textsuperscript{1134} Id.


\textsuperscript{1136} Id.


\textsuperscript{1138} Id.

currency. However, the SEC found that Centra Tech had no relationships with Visa or Mastercard. After a criminal investigation involving the same securities law violations, the co-founders were arrested in April 2018 and indicted by a grand jury in the Southern District of New York in May 2018. The U.S. Attorney’s Office and the FBI seized 91,000 Ether, which included digital funds raised during the ICO. At the time, the seized funds were worth more than $60 million.

On May 29, 2018, the SEC filed a complaint in the Central District of California against Titanium Blockchain Infrastructure Services, Inc. and its executives. The complaint alleges that the company engaged in the unregistered offer and sale of securities, and misled investors regarding the company’s relationships with the Federal Reserve and other well-known companies. The SEC also obtained a temporary restraining order halting the company’s ongoing ICO, which had already raised $21 million from investors both inside and outside of the United States.

8.4 Simple Agreement for Future Tokens

In the absence of any clear regulation from the SEC, many in the blockchain community have opined that ICO issuers should engage in responsible self-regulation. Protocol Labs, a decentralized Internet start-up, hopes to facilitate such responsible behavior through its CoinList and Simple Agreement for Future Tokens (SAFT). Announced in May 2017, CoinList is a platform developed for token-backed networks to raise money through token pre-sales. The platform uses SAFT, which is an investment instrument modeled on Y Combinator’s Simple Agreement for Future Equity (SAFE). In April 2018, three ICOs were launched through

---

1140 Id.
1141 Id.
1143 Id.
1144 Id.
1146 Id.
1147 Id.
CoinList’s platform – Filecoin, Blockstack and Prop. CoinList has raised $9.2 million to build out a platform where accredited investors can invest in ICO start-ups and open source projects. In 2013, Y Combinator, a start-up accelerator, released the SAFE investment instrument as an alternative to convertible debt. SAFE has now become the standard seed round investment agreement for small start-ups. While SAFE promises future equity, SAFT promises future tokens. CoinList will restrict its token presales to accredited investors. Investors will be accredited by AngelList, whose founder Naval Ravikant is an investor in Protocol Labs. The accreditation must conform with the SEC’s accredited investor requirements, which include either an annual income above $200,000 (or $300,000 together with a spouse) in each of the prior two years, or a net worth of over $1 million (whether alone or with a spouse).

SAFT is a Know Your Customer (KYC) enabled platform, meaning that every person on it is fully vetted to ensure compliance with all anti-money laundering (AML) and KYC requirements. Consequently, the SAFT requires that a considerable amount of information be taken from users, which makes it unappealing to blockchain anonymity purists. On the other hand, several facets of the agreement provide the flexibility and defensibility required for blockchain projects, whether or not they attract scrutiny from the SEC.

First, the greater securities compliance offered by the SAFT enables more widespread adoption. By giving accredited investors a platform for easy participation, crowdfunding becomes accessible to a much larger constituency. Second, such compliance provides more clarity for entrepreneurs. While CoinList does not guarantee protection from future regulation, it does provide easy steps to maintain securities compliance, thus avoiding the current confusion over the status of tokens as securities. Third, it facilitates offerings by foreign companies, who are subject to federal securities laws when offering tokens to U.S. investors. Under the SAFT, foreign companies could seek investment from accredited U.S. investors with some assurance that they were not violating securities laws.

1151 Id.
1152 Stephanie Zeppa & Andrew Kreider, SAFEs and KISSes Poised to Be the Next Generation of Startup Financing, Nat’l L. Rev. (May 6, 2015).
1154 Id.
1155 See generally Chapter 6.
SAFT has been the subject of criticisms, chiefly that the whitepaper generally only alters SAFE by substituting the word “tokens” for “equity.” Even so, it is a solid example of the blockchain community’s recognition that self-regulation of ICOs is paramount to the industry’s continued success and development.

8.4.1 Airdrops

Recently, blockchain companies have been conducting “airdrops” to gift tokens to participants in the crypto community. This practice involves pushing tokens into wallets that hold a particular type of cryptocurrency – typically bitcoin or Ether. Issuers generally engage in airdrops to create awareness about their ICO or tokens. This practice has recently been the subject of regulatory scrutiny, since the company engaging in the airdrop has no information about the recipients, other than a wallet address. To address regulators’ concerns, on April 25, 2018, CoinList announced a new product for airdrops that will process users through compliance checks and attestations before token issuers provide users with free tokens. Based on discussions with the SEC, CoinList’s CEO, Andy Bromburg, has expressed confidence that this platform complies with current regulations: “I can’t comment on individual discussions with the SEC. What I can say is we are in frequent communication with them and based on our understanding of securities law, we are very comfortable with this.”

8.5 International Developments

Prompted by the sharp increase in popularity of ICOs, several countries have released guidance on the applicability of their domestic securities laws to token offerings.

8.5.1 Canada

On August 24, 2017, the Canadian Securities Administrators (CSA) released a report indicating that a token issued in an ICO may be considered a security and that the test for determining this will be almost identical to the Howey test: whether there is an investment of money; in a common enterprise; with the expectation of profit; coming significantly from the efforts of others. Indeed, the only notable difference from the Howey test is the substitution of “significantly” for “solely” in the final prong.

---

1157 Rizzo, supra note 1149.
1159 Id.
1161 Id.
1164 Id.; Howey, 328 U.S. at 298-99.
If the ICO token meets the definition of a security, the issuer must ensure either that sales are made to accredited investors only through an offering memorandum prospectus exemption; or, where the ICO is trading in securities for a business purpose, the offering is registered with the CSA. The CSA report indicates that the ICO’s token is likely to be considered a security if the ICO’s promoters engage in the following: (1) soliciting a broad base of investors, including retail investors; (2) using the Internet, including public websites and discussion boards, to reach a large number of potential investors; (3) attending public events, including conferences and meet-ups, to actively advertise the sale of the coins/tokens; and, (4) raising a significant amount of capital from a large number of investors.

8.5.2 China

On September 4, 2017, the People’s Bank of China (PBoC) announced an immediate ban on ICOs. The PBoC cited concerns regarding the Chinese ICO industry, including, “the illegal sale of tokens; illegal securities issuance and illegal fundraising; financial fraud; pyramid schemes and other criminal activities.” The PBoC also stated that any organizations that have completed an ICO must make arrangements for repatriation of the funds in order to protect the interests of investors. Failure to comply with either directive could lead to criminal prosecution and punishment.

On September 18, 2018, the People’s Bank of China issued a new public notice reminding investors of the risk associated with ICOs and crypto trading. The notice reiterated that the “unauthorized” and “illegal” ICO financing model poses a “serious disruption” to the “economic, financial and social order.”

8.5.3 Hong Kong

On September 5, 2017, the Hong Kong Securities and Futures Commission (SFC) issued a statement explaining that certain tokens offered through ICOs have terms and features that may mean that they are “securities,” and these tokens may be regarded as an interest in a collective investment scheme. Accordingly, an ICO of such tokens may constitute a regulated activity, and any parties engaging in regulated activity targeting the Hong Kong public must be licensed or registered with the SFC irrespective of whether they are located in Hong Kong.

1165 NI 45-106 CSA § 2.9.
1167 Ontario Sec. Comm’n, supra note 1162.
The SFC issued another public warning in February of 2018, outlining the potential risks of ICOs and urging investors to do their due diligence.\footnote{Press Release, \textit{SFC Warns of Cryptocurrency Risks}, Hong Kong SEC (Feb. 9, 2018), \url{https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=18PR13}.} The SFC reiterated that it will continue to police cryptocurrency and ICO markets.\footnote{Id.}

\subsection*{8.5.4 United Kingdom}

On September 12, 2017, the United Kingdom’s Financial Conduct Authority (FCA) issued a warning that ICOs are high-risk, speculative investments. Among the FCA’s concerns: ICOs are not regulated by the FCA; there is no protection from the Financial Ombudsman or from the Financial Services Compensation schemes; the value of tokens is extremely volatile; there is potential for fraud; ICO whitepapers may be biased, incomplete or misleading; and most ICOs are early-stage projects and investors risk losing their whole stakes if the project fails. The FCA stated that the decision as to whether an ICO falls under FCA regulation will depend on whether the token is considered a security, which will be determined on a case-by-case basis.\footnote{Id.}

\subsection*{8.5.5 Thailand}

On May 13, 2018, the Thai government used an emergency decree to pass new legislation regarding cryptocurrencies. The Digital Asset Business Decree defines two types of digital assets, ‘cryptocurrencies,’ which are used as “a medium for exchanging goods, services or any other rights, or to be exchanged for other digital assets,” and ‘digital tokens,’ which are defined as “rights to take part in an investment or to receive specific goods.”\footnote{News Release, \textit{SEC Announces the Digital Asset Business Law Has Become Effective}, Thailand SEC (May 16, 2018), \url{https://www.sec.or.th/en/Pages/News/Detail_News.aspx?tg=NEWS&lg=en&news_no=50&news_yy=2018}.} The Decree sets forth that any digital asset business operators who are engaged in digital asset business activities must obtain permission from the Minister of Finance.\footnote{Id.} Existing digital asset business operators were required to obtain a license from the Minister of Finance by August 2018.\footnote{Id.}

\subsection*{8.5.6 South Korea}

On September 28, 2017, the Financial Services Commission of South Korea followed China’s example by issuing a ban on ICOs, citing the increased risk of financial scams and general regulatory uncertainty. A report by the commission stated that stern penalties would be levied on

any financial institutions or other parties involved in the issuance of ICOs. Speaking at the National Assembly’s annual audit on government actions, Hong Nam-Ki, head of the office for government policy coordination, announced that the South Korean government would soon make a decision on whether it will permit ICOs.

8.5.7 Germany

On February 20, 2018, Germany’s Federal Financial Supervisory Authority (BaFin) published a note on token regulation, explaining that it will consider tokens on a case-by-case basis, checking them for compliance against the Markets in Financial Instruments Directive II, the German Securities Prospectus Act, and the German Federal Ministry of Justice and Consumer Protection’s Investment Law, among other standards. BaFin is encouraging companies who are promoting tokens to determine whether their products or services fall under an existing regulation and to contact a specialist at BaFin with specific inquiries. The note also made clear that the mere designation of a token (i.e., utility token) is irrelevant to the outcome of the legal analysis.

8.5.8 Vietnam

After approximately 32,000 investors lost the equivalent of $658 million in two Vietnamese ICO scams, the Prime Minister announced that the Ministry of Justice would be assuming the primary responsibility for regulating ICOS and coordinating with other branches to propose and finalize the legal framework for handling virtual currency, assets and ICOs.

8.5.9 European Union

On November 13, 2017, the European Securities Market Authorities (ESMA) issued two statements on ICOs. The first warned investors of the “high risk of losing all of their invested capital” and that ICOs are very risky and speculative investments. The second statement

---


1180 *Id.*


addressed the relevant regulatory requirements for firms that deal with ICOs. ESMA explained that where ICOs qualify as financial instruments, it is likely that the conduct is regulated, in which case the firm needs to comply with relevant legislation, including the Prospectus Directive, the Markets in Financial Instrument Directive, the Alternative Investment Fund Managers Directive, and the Fourth Anti-Money Laundering Directive.\footnote{Id.}

\subsection*{8.5.10 Russia}

In April 2018, the Russian Ministry of Communications (MinCom) published an initial draft for ICO regulations, which provides that, for example, firms that facilitate token sale events will be required to guarantee that investors can sell their tokens back to those firms.\footnote{On Accreditation of Organizations Providing the Possibility of Issuing Digital Tokens, Government of the Russian Federation,  \url{http://regulation.gov.ru/projects#search=%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D1%8B%D0%B5&npa=79293}; see also Shiraz Jagati, Russian Government Prepares Stringent New ICO Regulations, Crypto Slate, (Apr. 3, 2018), \url{https://cryptoslate.com/russia-ico-regulations/}.} Accreditation requires the entity to: (1) be registered on the territory of the Russian Federation in accordance with current law; (2) have authorized capital of not less than 100 million rubles; (3) obtain a license issued by an authorized federal executive body for the development, production, and distribution of encryption (cryptographic) funds; (4) have an account open with a bank registered and licensed in accordance with the Russian Federation law on banking; and (5) have approved rules for issuing digital tokens.\footnote{Id.}

\subsection*{8.5.11 Singapore}

On November 14, 2017, the Monetary Authority of Singapore (MAS) released \textit{A Guide to Digital Token Offerings}. The guidance dictates that any ICOs that qualify as “capital market products”\footnote{Under Section 2(1) of the Securities Future Act, “capital market products” means any securities, futures contracts, contracts or arrangements for the purpose of foreign exchange trading, contracts or arrangements for the purposes of leveraged foreign exchange trading, and such other products as MAS may prescribe as capital market products.} under the Securities and Futures Act can be regulated by the MAS.\footnote{A Guide to Digital Token Offerings, Monetary Authority of Singapore (Nov. 14, 2017), \url{http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20%2014%20Nov%202017.pdf}.} This includes altcoins that can either infer an ownership interest in a corporation, product, debt, or a share in an investment structure. The Guide was updated in November 2018 to clarify that all intermediaries, which includes almost every participant involved in activities related to an ICO, must “take appropriate steps to identify, assess, and understand their money laundering and terrorism

\footnote{Id.}
financing (ML/TF) risks.” Intermediaries are expected to develop and implement internal policies under appropriate MAS notices that would allow the central bank to monitor customers’ due diligence and transactions, alongside financial records. Intermediaries must comply regardless of whether the token is classified as a security.

8.5.12 Switzerland

On February 16, 2018, the Swiss Market Supervisory Authority (FINMA) published a set of guidelines for the regulations of ICOs. FINMA will characterize ICO tokens as payment tokens, utility tokens, or asset tokens, and will assess the economic function and purpose of the tokens as well as whether they are tradeable or transferable.

8.5.13 Australia

In September 2017, the Australian Securities Investments Commission (ASIC) published an information sheet discussing how Australian law, particularly the Corporations Act of 2001, will impact ICOs. The information sheet specifies that if an ICO is classified as a financial product, then it is subject to the Corporations Act. If, however, the ICO is not a financial product, then it is subject to general laws and Australian consumer laws. ASIC encourages entities that are seeking to undertake an ICO or to issue a crypto-asset to carefully consider the nature of the ICO and the information being provided to consumers.

---

1189 Id.
1191 Id.
1193 Id.
1194 Id.
Chapter 9

9 Federal Banking Regulations

9.1 Electronic Funds Transfer Act (EFTA)

The Electronic Fund Transfer Act of 1978 (EFTA) was enacted to protect consumers who engage in electronic fund transfers (EFTs).1195 Implemented through the Federal Reserve Board’s Regulation E, the EFTA – along with this regulation – comprises a kind of “consumer bill of rights” for EFTs, setting forth the rights, financial liabilities, and obligations of both consumers and card issuers with respect to EFTs.1196

The EFTA defines EFTs as transfers of funds initiated through an electronic terminal, phone, computer (including online banking) or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer’s account.1197 EFTs include point-of-sale transfers, ATM transfers, direct deposits or withdrawals of funds, transfers initiated by telephone, and transfers resulting from debit card transactions, whether or not through an electronic terminal.1198 An ‘electronic terminal’ is defined as an electronic device through which a customer can initiate an EFT.1199

The first protection afforded by the EFTA and Regulation E is the requirement that a debit card issuer provide a method for identifying the customer to whom the card belongs.1200 The most common method is a magnetic strip or PIN number, but other examples include signature, fingerprint, or facial ID recognition.1201

The EFTA also protects consumers from liability in the instance of unauthorized use. Where a consumer immediately notifies a banking institution that a card has been lost or stolen, the consumer should incur zero liability for any subsequent unauthorized payments.1202 Where the card has been used to draw money before a report is filed with the financial institution, so long as the consumer informs the institution within two business days after learning of the loss or theft, the consumer’s liability is limited to $50.1203 If the institution is not notified within two business days, the consumer will be liable for up to $50 of loss that occurs in those first two days, plus any loss that occurs after such time up to $500.1204 To reach the limit, the institution must establish that the loss would not have occurred if the consumer had provided notification within two

1196 Id.
1197 12 C.F.R. § 205.3(b).
1198 Id.
1199 12 C.F.R. § 205.2(h).
1200 12 C.F.R. § 205.5(b)(4).
1201 Id.
1202 12 C.F.R. § 205.6(b)(1); Official Staff Commentary on Regulation E, § § 6(b), 6(b)(1).
1203 12 C.F.R. § 205.6(b)(2), 205.7(b)(1)-(3).
1204 Id.
business days. Unlimited loss liability can occur where an unauthorized transaction is not reported within 60 days and the institution can establish that the loss would not have occurred had notification been given.

Further, the EFTA places information disclosure requirements on card issuers mandating that they provide certain information such as: a) before the first transaction on the account, b) any time that an EFT is made at an ATM or other electronic terminal, and c) periodically, typically monthly. Initial disclosures include summaries of the consumer’s liability for unauthorized EFTs, the EFT services that are provided, and the relevant fees. When an EFT occurs, the issuer must provide a receipt that identifies the consumer’s account, the type and amount of the transfer, the date of the transfer, and the location of the terminal at which the transfer was made. The receipt can be used as evidence in judicial proceedings. Financial institutions must provide a periodic disclosure, usually in the form of a monthly statement, that must include specific information about the account and activity.

In 2009, the Federal Reserve amended Regulation E to prohibit financial institutions from charging overdraft fees for ATM and one-time debit charge transactions, except where the consumer opts in or affirmatively consents to the overdraft service. Shortly thereafter, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 transferred rulemaking authority under the EFTA from the Federal Reserve Board to the Consumer Financial Protection Bureau (CFPB). Considering that the CFPB has already warned consumers about the potential risks of transactions with virtual currency, the CFPB could very well rule that virtual currency is within its jurisdiction and apply the EFTA to virtual currency transactions.

---

1205 12 C.F.R. § 205.6(b)(2).
1206 12 C.F.R. § 205.6(b)(3).
1207 12 C.F.R. § 205.7.
1208 12 C.F.R. § 205.9(a).
1209 12 C.F.R. § 205.9(b).
1210 12 C.F.R. § 205.7(b). A terminal owner may charge for use of the terminal provided that the amount of the charge is displayed on the terminal or disclosed on the receipt. 12 C.F.R. § 205.9(a).
1211 12 C.F.R. § 205.9(a).
1213 12 C.F.R. § 205.9(b).
1216 See generally Chapter 10 (Consumer Protection), supra.
If this occurs, virtual currency exchange sites may be required to comply with the same liability and disclosure requirements as banks. For example, there is currently no protection if a consumer’s virtual currency is lost or stolen. If the EFTA requirements apply to virtual currency, however, any lost or stolen currency would have to be replaced by the exchange within a set number of days after the consumer discloses the loss. While this requirement may potentially be onerous for virtual currency exchanges, consumer protection rules of this sort should make virtual currency more attractive to first-time users.

9.1.1 Prepaid Accounts Rule Exempts Virtual Currency

Originally, the EFTA did not apply to prepaid accounts. On October 5, 2016, however, the CFPB issued new guidance concerning prepaid card products and prepaid accounts.1217 In a Notice of Proposed Rulemaking, the Bureau announced its intention to bring prepaid accounts within the ambit of Regulation E.1218 The definition of ‘prepaid accounts’ would include cards, codes, devices capable of being loaded with funds that are usable at unaffiliated merchants, or for person-to-person transfers, excluding gift cards.1219

Any companies issuing such products would be required to provide certain disclosures to consumers before and after the acquisition of a prepaid account, as required under EFTA, and Regulation E’s limited liability and error resolution provisions would apply to prepaid accounts.1220 A statement of the prepaid account’s terms and conditions would have to be registered with the Bureau and made available on the company’s website.1221 The Notice expressly stated that “the proposed rule may have potential application to virtual currency and related products and services.”1222

During the public comment period, the CFPB received many comments in response to the Bureau’s statement that the proposed rule might apply to virtual currency services.1223 One hundred and fifty comments were received from a wide range of interested parties, including

1218 Id.
1220 Id.
1221 Id.
1223 Id.
banks, digital wallet providers, currency exchanges, consumer advocacy groups, and others. For example, Coin Center, a non-profit organization focused on policy issues relating to cryptocurrencies, filed a comment contending that procedural fairness dictated that the proposed rule should not apply to virtual currency. More specifically, Coin Center argued that the CFPB had not adequately studied the cryptocurrency industry to determine how existing rules would affect cryptocurrency products; that the small scale of the virtual currency industry relative to traditional prepaid products made the application of the rules slightly less urgent; and that the intricacies of cryptocurrency technology required further study and consideration. Coin Center stressed that the decentralized nature of virtual currencies provides some inbuilt consumer protection due to transparency and open-source architecture. Predictably, consumer-group commenters generally urged the Bureau to regulate virtual currency.

Ultimately, when the final rule was announced, the CFPB clarified that virtual currency would not fall under the ambit of prepaid accounts. The CFPB concluded that the application of Regulation E to the prepaid accounts rule was beyond the scope of its final rulemaking, but that it would continue to analyze the nature of services tied to virtual currencies. Many in the industry are bracing for a new set of regulations, as complaints about “virtual currency” increased from seven in 2016 to 277 in 2017.

9.1.2 The Consumer Financial Protection Bureau’s Sandbox

In July 2018, the CFPB launched a FinTech regulatory sandbox to encourage consumer-friendly innovation, creation of policies to facilitate innovation, engagement with entrepreneurs and regulators, and review of outdated or unnecessary speculations. The interim director of the CFPB, Mike Mulvaney, indicated that he expects those involved to look closely at emerging financial technologies, including blockchain and cryptocurrency. Many critics of the sandbox
claim that the CFPB’s goal is less about providing start-ups with a testing ground than about helping the agency determine how to regulate emerging cryptocurrencies and blockchain technology.1232

9.2 Federal Reserve

The Federal Reserve System (also known as the “Federal Reserve” or “Fed”) was established on December 23, 1913, as a third attempt at central banking in the United States. Outbreaks of financial instability, known as “panics,” occurring in the late 19th and early 20th centuries prompted Congress to establish the National Monetary Commission in 1908 to study their underlying causes and recommend a solution.1233 After several years of research and debate, Congress approved and President Woodrow Wilson signed the Federal Reserve Act of 1912 into law, creating what we now know as the modern U.S. central banking system, the Federal Reserve, in 1913.1234

Great care was taken in drafting the Federal Reserve Act to develop a central banking system that would provide the nation with a safer, more flexible, and more stable monetary and financial system. While the Federal Reserve System did not prevent the Great Depression or the Global Financial Crisis, and its policies do, at times, aggravate inflation, most still believe that some federal control over private banking is needed to prevent the bank suspensions and failures that brought such instability to the economy leading up to 1914.

The Fed supervises and regulates state member banks (i.e., state chartered banks that have chosen to become members of the Federal Reserve) and bank and financial holding companies (i.e., companies that own banks).1235 The Fed also supervises overseas and international operations of regulated financial institutions.1236 Foreign banks with U.S. branches, agencies and nonbank operations are also subject to Fed’s supervision.1237 Other financial institutions, such as nationally chartered banks, are supervised by other entities, such as the Office of the Comptroller of the Currency.1238 The Fed’s Banking Supervision and Regulation units work closely with other

1234 Id.
regulators and authorities to ensure that regulations are uniformly applied and consistently enforced throughout the banking system.

The Federal Reserve fulfills its supervisory responsibilities through a wide range of activities, including:

- Distributing supervisory and regulatory guidance documents to financial institutions’ management and directors;
- Reviewing and approving applications for new member banks, bank mergers, and other organizational changes;
- Conducting on-site examinations and inspections of state member banks, foreign banking organizations, and bank and financial holding companies;
- Meeting with management and directors of financial organizations;
- Monitoring and surveillance of bank performance and activities;
- Tracking conditions in the banking sector of the national economy;
- Identifying specific areas of emerging risks; and
- Initiating enforcement actions, when warranted.1239

9.2.1 Federal Guidance

9.2.1.1 Federal Advisory Council and Board of Governors (5-9-2014)

On May 9, 2014, the Federal Advisory Council met with the Board of Governors of the Federal Reserve to discuss the current condition and outlook for loan markets and financial markets in general.1240 One item on the docket for discussion was bitcoin and whether the cryptocurrency poses a threat to the banking system, economic activity, or financial stability.1241 Concerns about bitcoin included the disruption of traditional payment networks and traditional channels of commerce, the potential for shadow transacting and illicit use, and the potential to act as a catalyst of instability through volatility and network failures.1242

While the council initially acknowledged that bitcoin posed no imminent threat to the banking industry, the council forecasted that bitcoin may have a long-term impact due to aspects of the currency that appeal to merchants, including lower transaction fees, cheap international

1242 Id.
exposure to the developing world, faster settlements, and geographic flexibility. The council warned that the banking industry’s adoption of the technology would be hindered by security concerns (e.g., the lack of deposit insurance in cases like Mt. Gox) and the unpredictability of virtual currency’s value. Further, while the council maintained there were multiple potential illicit applications for bitcoin, it acknowledged that bitcoin presents no threat to economic activity and could, in fact, be a boon due to its global transmissibility and ability to drive capital to the developing world.

The council decided that regulation is advisable to protect consumers, address illicit use, and avoid balkanization. Regarding consumer protection, the council advised that susceptibility to theft must be addressed through supervised risk management of currency exchanges and regulatory oversight to ensure that appropriate cybersecurity measures are in place both in exchanges and on wallet storage sites. As for illicit use, the council proposed that anti-money laundering (AML) and Know Your Customer (KYC) policies be implemented to prevent trafficking in bitcoin, and that suspicious activity reports be utilized to enable monitoring and pattern recognition. To avoid balkanization, the council called for consistency across geographic areas to preempt regulatory arbitrage. The council stated that, while they expect bitcoin advocates to argue that regulation minimizes decentralization, recent events dictated that some flexibility be sacrificed to address obvious problems.

9.2.1.2 Strategies for Improving U.S. Payment Systems

On January 26, 2015, the Federal Reserve released a paper on strategies for improving U.S. payment systems, calling on stakeholders to join together to help. The paper identified five key goals: (1) speedy electronic solutions for making a broad variety of business or personal payments, (2) secure systems that remain strong and maintain public confidence, (3) efficient systems with more payments placed electronically to reduce societal costs of payment transactions and enable

---

1243 Id.
1244 Id.
1245 Id. at 11.
1246 Balkanization generally refers to the division of a large element into smaller units. With respect to the internet and technology, balkanization refers to the raising of virtual borders in a space that was intended to be a vehicle for sharing knowledge without regard for national borders, often through means of including restricting innovation. Rich Cooper, Say No to the Balkanization of the Internet, U.S. Chamber of Commerce Foundation (Mar. 30, 2015) https://www.uschamberfoundation.org/blog/post/say-no-balkanization-internet/42923.
1247 Id.
1248 Id.
1249 Id.
innovative services, (4) better choices for convenient cross-border international payments, and (5) systems that are collectively embraced by a broad array of participants.1251

The paper made several specific suggestions for how the Federal Reserve could achieve these general outcomes:

- Actively engage stakeholders on initiatives to improve the U.S. payment system, for example, by seeking strategic input from stakeholders and providing opportunities for stakeholder feedback and engagement.1252

- Identify approaches for implementing safe, ubiquitous, and faster payments through establishing a Faster Payments Task Force, examining policy issues related to multi-provider environments, and supporting collective stakeholder efforts.1253

- Reduce fraud risk and advance the safety, security and resiliency of the payment system by establishing a Payment Security Task Force to coordinate with the Faster Payments Task Force.1254

- Achieve greater efficiency in cross-border payment systems by developing a strategy for the application of the ISO 200221255 standard to U.S. payment transactions and developing technologies and rules that foster interoperability for P2P and B2B payments.1256

- Enhance Federal Reserve Bank payments by expanding the operating hours of the National Settlement Service and accelerate interbank settlement for checks, to promote use of same-day ACH capabilities, to expand risk management services for Federal Reserve Financial Services, and to provide the Reserve Banks’ network of financial institution customers with access to interoperable, secure directory tools.1257

Since its inception, the Faster Payments Task Force has published a major research report in two parts, the first of which was released in January 2017 and the second in July of that same year. The first part describes the background and process of the task force’s work, with the intent

1251 Id. at 2.
1252 Id. at 3.
1253 Id.
1254 Both task forces were charged with determining areas of focus and supporting the evolution and adoption of appropriate standards. Further, the Federal Reserve’s suite of anti-fraud and risk-management services would be used to enhance payment services, with improvements being made to the Federal Reserve’s publicly available payment fraud data. Id.
1255 The International Standards Organization developed the ISO 20022 standard for financial messaging.
1257 Id. at 5.
to encourage proposals for faster payment solutions. The report emphasizes that most consumers are transacting via electronic payment methods, and suggests that future proposals focus on providing new opportunities for payment providers to implement user-friendly and safe electronic transactions. Citing a June 2016 BAI study, the report praises trends like mobile device applications, application programming interfaces (APIs), Internet of Things (IoT) devices, digital currencies, and distributed ledger technology. Specifically, the report acknowledges that digital currencies have potential to change the payments landscape and that distributed ledger technology may change the roles of traditional players in the payment clearing and settlement processes (e.g., by eliminating the need for centralized transaction bookkeeping).

In July 2017, the Faster Payments Task Force released the second part of its report, which outlines the proposals it received, considers foundational issues requiring collaborative action, and recommends further measures to achieve faster payment systems. The report provides an overview of sixteen different proposals, five of which use a blockchain, distributed ledger technology, or virtual currency. Proposals came from existing virtual currency business Ripple, Thought Matrix Consulting, LLC, and Wingcash — each of which proposed that the Federal Reserve issue its own virtual currency. The paper concludes with recommendations for continuing research and analysis of several proposed solutions, including digital currencies and distributed ledger technologies. It states that the task force requires a greater understanding of the risks posed by distributed ledger technologies and wants to review research on enhancing security and meeting unmet needs in cross-border transactions among underserved end users.

In June 2018, Ryan Zagone, Ripple’s Director of Regulatory Relations, was elected to the Faster Payments Task Force Steering Committee.

---

1259 Id. at 25.
1260 Id. at 23 (citing BAI Consumer Market Pulse Survey (Jun. 2016)).
1261 Id.
1262 Faster Payments Task Force supra note 1258, at 23.
1264 Id. at 9-14.
1265 Id. at 52.
1266 Id. at 29.
1267 Id.
On September 6, 2017 the Federal Reserve released a progress report providing refreshed strategies and tactics. The Federal Reserve claimed that good progress has been made toward achieving the five outcomes, and noted that private sector providers have helped significantly by designing and introducing technology that allows faster payment. Critically, the board announced that, following the initial report, the payment industry began exploring potential uses of virtual currency and distributed ledger technology for delivering faster payment solutions. The report concluded with three new suggestions: supporting a collaboration work group to develop a faster payments ecosystem; pursuing settlement services to address future needs for ubiquitous real-time retail payments; and assessing the need for the Federal Reserve’s engagement as a service provider. The Federal Reserve also stated its intent to study and solicit input from stakeholders on virtual currencies and distributed ledger technology.

9.2.1.3 Distributed Ledger Technology in Payments, Clearing and Settlement

In 2016, Federal Reserve staff researchers published a paper on distributed ledger technology (DLT) in payments, clearing, and settlement. The paper discusses potential uses for DLT in those areas, analyzes industry approaches to adopting DLT, and discusses challenges to adoption, including financial risks and legal considerations. It cites potential uses of DLT, including the opportunity to provide new ways to transfer and record ownership of virtual assets, to immutably store information, and to provide identity management and other evolving operations through P2P networking.

9.3 The Office of the Comptroller of the Currency (OCC)

The Office of the Comptroller of the Currency (“OCC”) has authority to charter national banks and special purpose banks that engage in “the business of banking.” The OCC has interpreted this term to encompass banks that engage in fiduciary activities or that receive deposits, pay checks, or lend money. In December 2016, the OCC published a whitepaper titled

---

1270 Id. at 2.
1271 Id. at 7.
1272 Id.
1274 Id. at 17
1275 Id. at 27.
1276 Id. at 34.
1278 12 C.F.R. § 5.20(e)(1).
“Exploring Special Purpose National Bank Charters for FinTech Companies,” in which it proposed issuing special purpose national bank (SPNB) charters to financial technology companies that engage in the business of banking (the “FinTech Charter”).

The OCC reasoned that, because it has “legal authority to construe these activities to include bank-permissible, technology-based innovations in financial services,” it further has authority to issue FinTech Charters. In March 2017, the OCC issued a draft supplement to its Licensing Manual “explain[ing] how the OCC will apply the licensing standards and requirements in existing regulations and policies to FinTech companies applying for special purpose national bank charters.”

Pursuant to the draft supplement, an entity that intends to engage in one of the core banking activities (i.e., receiving deposits, paying checks, or lending money) may apply for a FinTech Charter. The supplement interprets these terms broadly to encompass activities such as discounting notes, purchasing bank-permissible debt securities, engaging in lease-financing transactions, making loans, issuing debit cards, or engaging in other means of facilitating payments electronically. The supplement encourages interested entities to communicate with the OCC before filing an application to discuss whether a proposed activity falls within the scope of the agency’s authority.

According to the draft supplement, in evaluating a FinTech Charter application, the OCC considers whether the proposal is unfair or deceptive, or poses an undue risk to consumers, as well as whether the proposal would result in the commingling of banking and commercial activities. The OCC also considers whether the entity has: (1) management with appropriate skills and experience; (2) adequate capital to support projected volume and type of business and proposed risks; and (3) a comprehensive business plan, including financial projections, analysis of risks, and

---


1280 Id.


1283 Id.

1284 Id.

1285 Id.
risk management controls. The OCC may also impose special conditions if it identifies any requirements necessary for the success of the business. 1286

Currently, the OCC’s authority to issue FinTech Charters is being challenged in two separate cases. On April 26, 2017, the Conference of State Bank Supervisors (CSBS)1287 filed a complaint against the OCC arguing that the agency had exceeded its authority under the National Bank Act, which limits OCC charters to entities engaged in the “business of banking.” 1288 The CSBS argued that Congress had intended that phrase to mean “deposit taking,” meaning that the OCC’s expansive interpretation — i.e., that its authority extended to any entities engaged in fiduciary activities or activities, including paying checks or lending money — was improper.1289 The CSBS also claimed that the OCC had failed to follow proper rulemaking procedures under the Administrative Procedure Act, and that the FinTech Charter was preempted by the Supremacy Clause and Tenth Amendment.1290

On July 28, 2017, the OCC filed a motion to dismiss, arguing that the CSBS lacked standing and that the case was unripe because the agency had yet to decide whether to make the charters available to FinTech companies.1291 The OCC also argued that the CSBS complaint had failed to state a claim, as the OCC’s reasonable interpretation of its authority to regulate “the business of banking” under the NBA is entitled to deference under Chevron, U.S.A., Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837 (1984).1292 On April 30, 2018, the court granted the OCC’s motion to dismiss on the grounds that CSBS lacked standing to sue because the OCC had yet to officially decide whether it would issue charters to FinTech companies.1293 The court

---

1286 Id.
1287 The CSBS is a nationwide organization of banking and financial services regulators from all 50 U.S. states, the District of Columbia, and U.S. territories.
1290 Id.
1292 Id.
also ruled that the case was unripe for consideration since CSBS was unable to establish an injury in fact.\textsuperscript{1294}

Similar to the CSBS complaint, on May 12, 2017, the New York Department of Financial Services filed suit against the OCC, arguing that the issuance of the proposed FinTech Charter would violate the NBA and Tenth Amendment.\textsuperscript{1295} On August 18, 2017, the OCC moved to dismiss, raising the same arguments it had made in opposition to the CSBS complaint. On December 12, 2017, the court granted OCC’s motion, ruling that the plaintiff lacked standing because the OCC had not reached a final decision on the FinTech Charter.\textsuperscript{1296}

On July 31, 2018, the OCC announced that it would begin accepting applications for national bank charters from non-depository FinTech companies engaged in the business of banking.\textsuperscript{1297} The OCC announcement stressed the following:

- Every application will be evaluated on its unique facts and circumstances.
- FinTech companies that apply and qualify for, and receive, special purpose national bank charters will be supervised like similarly situated national banks, including capital, liquidity, and financial inclusion commitments as appropriate. FinTech companies will be expected to submit an acceptable contingency plan to address significant financial stress that could threaten the bank’s viability. The plan should outline strategies for restoring the bank’s financial strength and options for selling, merging, or liquidating the bank in the event that recovery strategies are ineffective.
- The expectations for promoting financial inclusion will depend on the company’s business model and the types of planned products, services, and activities.
- New FinTech companies that become special purpose national banks will be subject to heightened supervision initially, similar to other \textit{de novo} banks.
- The OCC has the authority, expertise, processes, procedures, and resources necessary to supervise FinTech companies that become national banks and to unwind a FinTech company that becomes a national bank in the event that it fails.\textsuperscript{1298}

The announcement also specified that eligible FinTech companies could also apply for federal charters under the OCC’s authority to charter full-service national banks and other special

\textsuperscript{1294} Id.


\textsuperscript{1298} Id.
purpose banks, such as trust banks, banker’s banks, and credit card banks. Many speculate that this announcement will cause states to revive their previous challenges to the OCC’s FinTech Charter.

---

1299 *Id.*

Chapter 10

10 Consumer Protection

The vast and complex economy of the United States is fertile ground for a wide range of innovative products and services. With such opportunity, however, come risks of fraud, scams, and theft. Businesses large and small can take advantage of their market power to deceive and exploit consumers. In the United States, consumers’ rights and interests are generally protected under common law and federal and state statutes.

10.1 State Law

Every state has practices to protect consumers from unscrupulous business practices and laws prohibiting unfair and deceptive acts. Consumer protection statutes provide the basic safeguards for the millions of everyday transactions that consumers enter into each year. Unfair and deceptive acts statutes are primarily civil statutes, with some authorizing criminal penalties for extreme violations. Typically, such statutes allow a state enforcement agency, most commonly the state’s Attorney General, to seek an order prohibiting a business from engaging in an unfair or deceptive practice. The agency can then seek an imposition of civil penalties for violations and an order to return a consumer’s payments. Further remedies include temporary or permanent injunctions to prevent repeat fraudulent practices.

Most states provide a broad prohibition on deceptive practices, including both deceptive and unfair acts, which is enforceable by consumers. This broad prohibition can include harassment, high-pressure sales tactics, and unfair bargaining of contract terms, even where the deception is not explicit. This affords consumers the highest level of protection and allows courts and enforcement agencies to determine unfairness on a case-by-case basis. Several states include no general prohibition and instead provide only a list of specific deceptive practices, including Colorado, Indiana, Iowa, Mississippi, Michigan, Oregon, Rhode Island, South Dakota, and Texas. Consequently, these states are not as consumer-friendly as the others. Additionally, the Michigan and Rhode Island state supreme courts have gutted their consumer protection statutes to the point that they apply to almost no consumer transactions.

While the laws differ from state to state, their basic premise reflects the Federal Trade Commission Act’s position, as discussed below, that unfair and deceptive tactics are inappropriate in the marketplace. Considering the similarities between federal and state laws, enforcement actions against violators are often jointly pursued by the Federal Trade Commission and a state’s Attorney General.

\[1301\] Carolyn Carter, Consumer Protection in the States, Nat’l Consumer Law Ctr. 9 (Feb. 2009).
\[1302\] Id.
\[1303\] Id. at 11
10.2 Federal Law

10.2.1 The Federal Trade Commission Act of 1914

The Federal Trade Commission Act \(^{1305}\) of 1914 (FTCA) created the Federal Trade Commission (FTC) to prevent anti-competitive acts \(^{1306}\) as part of the battle to “bust the trusts.”\(^{1307}\) Subsequently, Congress expanded the agency’s authority to regulate anticompetitive practices.\(^{1308}\) In 1938, Congress passed a prohibition against unfair and deceptive acts or practices.\(^{1309}\) In 1975, Congress gave the FTC the authority to adopt industry-wide trade regulation rules.\(^{1310}\)

The FTC is empowered to, among other things, issue cease and desist orders,\(^{1311}\) file civil actions,\(^{1312}\) investigate individuals and businesses,\(^{1313}\) and promulgate rules.\(^{1314}\) The FTC may compel testimony from witnesses and production of documents by issuing subpoenas\(^{1315}\) or civil investigative demands.\(^{1316}\)

In June 2015, the FTC’s Office of Technology Research and Investigation (OTRI) released an advisory statement on the use of bitcoin.\(^{1317}\) Specifically, the OTRI warned that bitcoin posed large risks due to its price fluctuations, irreversibility, and lack of legal protections as compared to traditional methods of payment.\(^{1318}\) The OTRI stated it had received “hundreds of complaints

\(^{1305}\) 15 U.S.C. § 41 et seq.

\(^{1306}\) 15 U.S.C. § 45(a)(2) (“The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations … from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.”).


\(^{1311}\) 15 U.S.C. § 45(b)-(g).

\(^{1312}\) 15 U.S.C. § 45(m).


\(^{1316}\) Civil investigative demands are similar to subpoenas but also allow the FTC to require recipients to file written reports or answers to questions. 15 U.S.C. § 57b-1.


\(^{1318}\) Id.
involving bitcoins and other virtual currencies,” with consumers generally complaining about online merchants who had failed to deliver a product or had given refunds in store credit rather than currency. The OTRI advised consumers to research a seller’s reputation before making purchases with virtual currency, and to research whether payment goes through a payment processor, possibly offering some protection and refunds.

Since then, the FTC has provided additional warnings to consumers regarding cryptocurrency and cryptocurrency scams. For example, in June 2018, the FTC announced that consumers had lost $532 million to cryptocurrency-related scams in the first two months of 2018 and that the agency expects that number to surpass $3 billion by the end of 2018.[1322] On June 25, 2018, the FTC held an event titled Decrypting Cryptocurrency Scams at which consumer groups, law enforcement agencies, research organizations, and the private sector explored how scammers are exploiting public interest in cryptocurrencies and ways to empower and protect consumers.[1323] In August 2018, the FTC warned of scammers sending letters to consumers threatening to expose allegedly damaging personal secrets unless the consumer pays a “confidentiality fee” in bitcoin.[1324]

10.2.1.1 Unfair Methods of Competition and Unfair or Deceptive Acts or Practices

The FTCA prohibits “[u]nfair methods of competition in or affecting commerce,”[1325] but does not define what constitutes an unfair method of competition. The FTC, however, has clarified that the prohibition encompasses not only violations of the Sherman and Clayton Antitrust Acts[1326] but also any act or practice that “cause[s], or [is] likely to cause, harm to competition or the competitive process, taking into account any associated cognizable efficiencies and business justifications.”[1327]

1319 Id.
1320 Id.
1321 Id.
The FTCA also prohibits “unfair or deceptive acts or practices in or affecting commerce.”\textsuperscript{1328} To be unfair or deceptive, the act must be one that “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or to competition.”\textsuperscript{1329}

10.2.1.2 Enforcement

The FTC is empowered to prevent any persons, partnerships, or corporations, except banks, savings and loan institutions, credit unions, and common carriers, from “using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.”\textsuperscript{1330}

In September 2014, the FTC filed a complaint against Butterfly Labs, a developer of bitcoin mining computers, and three of its officers, alleging that the defendants had engaged in deceptive business acts and practices in violation of the FTCA by, among other things, refusing to provide refunds to consumers who had paid for mining equipment but never received it.\textsuperscript{1331} In February 2016, the company and two of the individual defendants settled with the FTC.\textsuperscript{1332} One defendant agreed to a judgment of $135,878, part of which was satisfied by liquidating bitcoin in that defendant’s possession, with the remainder being suspended due to inability to pay.\textsuperscript{1333} The company and the other individual defendant agreed to a judgment of $38,615,161, of which they paid $19,000, with the remainder being suspended due to inability to pay.\textsuperscript{1334}

In June 2015, the FTC and the state of New Jersey filed charges against a mobile phone app developer for violations of the FTCA and New Jersey’s consumer fraud act, alleging that the defendant had sold an app containing malware that took control of a consumer’s mobile device to mine for virtual currencies, such as Dogecoin, Litecoin, and Quarkcoin.\textsuperscript{1335} The defendant settled with the FTC, agreeing to cease creating and distributing malicious software, to destroy consumer

\textsuperscript{1329} 15 U.S.C. § 45(n).
\textsuperscript{1330} 15 U.S.C. § 45(a)(2).
\textsuperscript{1331} Compl. for Permanent Inj. and Other Equitable Relief, \textit{Federal Trade Commission v. BF Labs, Inc.}, No. 4:14-cv-00815-BCW (WD Mo. Sept. 15, 2014).
information obtained in connection with the mobile phone app, and to pay a judgment of $50,000, most of which would be suspended upon payment of $5,200 to the state of New Jersey and compliance with the injunctive provisions of the stipulated order.\footnote{Press Release, Federal Trade Commission, App Developer Settle FTC and New Jersey Charges It Hijacked Consumers’ Phones to Mine Cryptocurrency (Jun. 29, 2015), https://www.ftc.gov/news-events/press-releases/2015/06/app-developer-settles-ftc-new-jersey-charges-it-hijacked.}

On February 20, 2018, the FTC filed a complaint against Thomas Dluca, Louis Gatto, Erik Pinkerson and Scott Chandler, for their involvement in “chain referral” schemes, including Bitcoin Funding Team and My7Network.\footnote{Compl. for Permanent Injunction and Other Equitable Relief, Federal Trade Commission v. Thomas Dluca, et al., No. 18-cv-60379 (Feb. 20, 2018) https://www.ftc.gov/system/files/documents/cases/dluca_bitcoint_funding_team_complaint.pdf.} The FTC alleges that defendants used various social media platforms to promise investors big rewards for a small payment of bitcoin or Litecoin.\footnote{Id.} Participants could only generate revenue by recruiting new participants and convincing them to also pay in cryptocurrency.\footnote{Id.} The complaint further claims that the defendant, Scott Chandler, who also promoted another scheme called Jetcoin, promised investors that they could double their investment within 50 days through bitcoin trading.\footnote{Id.} All defendants were charged with violating the FTC’s prohibition against “deceptive acts by misrepresenting the chain referral schemes as \textit{bona fide} money-making opportunities and by falsely claiming that participants could earn substantial income by participating in these schemes.”\footnote{Id.} On March 16, 2018, the United States District Court for the Southern District of Florida issued a temporary restraining order and froze defendants’ assets pending trial.\footnote{Press Release, Federal Trade Commission, FTC Shuts Down Promoters of Deceptive Cryptocurrency Schemes (Mar. 16, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/ftc-shuts-down-promoters-deceptive-cryptocurrency-schemes.}

\subsection{10.2.1.3 FTC’s Blockchain Working Group}

On March 16, 2018 the FTC created a Blockchain Working Group to identify and target fraudulent schemes that implicate the FTC’s consumer protection and competition missions.\footnote{Neil Chilson, It’s Time for a FTC Blockchain Working Group, Federal Trade Commission (Mar. 16, 2018), https://www.ftc.gov/news-events/blogs/techftc/2018/03/its-time-ftc-blockchain-working-group.} The working group has three main goals: (1) building “FTC staff expertise in cryptocurrency and blockchain technology through resource sharing and by hosting outside experts”; (2) assisting in “internal communication and external coordination on enforcement actions”; and (3) providing a
“forum for discussing potential influences on the FTC’s objectives and how to respond to them.”

10.2.2 The Dodd-Frank Wall Street Reform and Consumer Protection Act

The Dodd-Frank Wall Street Reform and Consumer Protection Act1345 (Dodd-Frank Act) was enacted in July 2010, making significant changes to financial regulation in response to the financial crisis of 2007-08. Among these reforms, the Dodd-Frank Act established the Consumer Financial Protection Bureau1346 (CFPB), an independent agency within the Federal Reserve, with the purpose of ensuring that “all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive.”1347 In particular, the CFPB’s objective is to ensure that, with respect to consumer financial products and services:

- Consumers are provided with timely and understandable information to make responsible decisions about financial transactions;
- Consumers are protected from unfair, deceptive, or abusive acts and practices and from discrimination;
- Outdated, unnecessary, or unduly burdensome regulations are regularly identified and addressed in order to reduce unwarranted regulatory burdens;
- Federal consumer financial law is enforced consistently, without regard to the status of a person as a depository institution, in order to promote fair competition; and
- Markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation.1348

The Dodd-Frank Act authorizes the CFPB to conduct investigations and issue subpoenas and civil investigative demands,1349 to issue cease and desist orders,1350 and to commence civil actions for civil penalties or legal and equitable relief.1351 To accomplish its objectives, the CFPB is authorized to enforce proceedings against entities in violation of consumer protection laws. Where the CFPB is made aware of a violator, whether through consumer complaints or more direct investigatory work, its Office of Enforcement recommends whether to commence enforcement

1344 Id.
1347 12 U.S.C. § 5511(a). The Dodd-Frank Act has an extensive definition of “consumer financial product or service,” which includes the extension of credit, the engagement of deposit-taking activities, the transmission or exchange of funds, and the sale of stored value or payment instruments, all for personal, family, or household purposes. 12 U.S.C. § 5481(5), (15).
Proceedings, and, depending on the subject violations, whether the Bureau should offer the alleged violator the opportunity to submit a written statement of explanation.\(^\text{1352}\)

The decision of whether to provide a violator the opportunity to write an explanatory statement is discretionary and typically inappropriate in cases of ongoing fraud or where the Office of Enforcement needs to act quickly.\(^\text{1353}\) Where the explanation is deemed insufficient, the Dodd-Frank Act authorizes the CFPB to apply to the United States District Court within the jurisdiction of the subject’s principal place of business, for the purposes of enforcing a bulletin, notice, or order, and to file civil cases for violations of the Act.\(^\text{1354}\) The CFPB is authorized to seek civil penalties or equitable relief, including permanent and temporary injunctions.\(^\text{1355}\)

In August 2014, the CFPB issued a consumer advisory warning about the risks associated with virtual currencies, such as threats from hackers, fewer protections by companies, higher costs and hidden fees, and fraudulent schemes.\(^\text{1356}\) The CFPB, however, has yet to issue any regulations concerning virtual currencies.

The CFPB maintains a consumer complaint database,\(^\text{1357}\) which shares certain data about consumer complaints and company responses thereto. In September 2016, the CFPB populated the database with information on consumer complaints regarding virtual currency products.\(^\text{1358}\) The database includes hundreds of complaints concerning virtual currency products for various issues, such as fraud, unavailability of money when promised, confusing or missing disclosures, and miscellaneous transaction or service problems.\(^\text{1359}\) Even so, the CFPB has yet to take any enforcement action against virtual currency companies for violations of federal consumer financial laws.

**10.2.3 The Gramm-Leach-Bliley Act**

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, along with its implementing regulations, governs a financial


\(^{1353}\) Id.


\(^{1358}\) Id.

institution’s treatment of nonpublic personal information (“NPI”). The GLBA requires financial institutions to safeguard NPI and prohibits them from sharing a consumer or customer’s NPI with a nonaffiliated third-party without first giving notice and an opportunity to opt out. The GLBA does not supersede or alter state laws, and states are free to enact laws providing even greater protection.

The GLBA originally granted rulemaking and enforcement authority to a variety of federal and state financial regulatory agencies, including the Office of the Comptroller of Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Board of Governors of the Federal Reserve System (Board), National Credit Union Association (NCUA), Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), and the former Office of Thrift Supervision (OTS), which merged with the OCC in 2011. In 2000, the OCC, FDIC, Board, and other federal regulators published regulations that are commonly referred to as the Privacy Rule, implementing sections 6802 and 6803 of Title 15. In 2001, these agencies also issued guidelines for safeguarding customer information (commonly referred to as the Safeguard Rule), which implemented section 6801 of Title 15.

In 2010, the Dodd-Frank Act generally transferred rulemaking and enforcement authority for the privacy provisions of the GLBA (15 U.S.C. §§ 6802-6809) to the CFPB. In December

---

1366 12 U.S.C. §§ 5481(12)(J), 5514(b)-(c), 5515(b)-(c); 15 U.S.C. §§ 6801(b), 6804(a)(1)(A), 6805. Pursuant to the GLBA privacy policy disclosure provisions, the FTC generally retains rulemaking authority for motor vehicle dealers predominantly engaged in the sale and servicing of motor vehicles, the leasing and servicing of motor vehicles, or both. 15 U.S.C. § 6804(a)(1)(C). Additionally, the SEC has rulemaking authority over securities brokers and dealers, investment companies, and investment advisers registered with the SEC under the Investment Advisers Act of 1940. And CFTC has rulemaking authority over futures commission merchants, commodity trading advisors, commodity pool operators, and introducing brokers subject to the CFTC’s jurisdiction under the Commodity Exchange Act with respect to any
2011, the CFPB republished the Privacy Rules previously adopted by the other federal agencies as interim final rules, with only certain technical and conforming changes;\textsuperscript{1367} and, in April 2016, the CFPB adopted the IFRs as final rules.\textsuperscript{1368} The Dodd-Frank Act, however, did not transfer to the CFPB rulemaking and enforcement authority concerning the information security safeguard provisions, and the Safeguard Rules adopted by the various federal agencies (i.e., the NCUA, OCC, Board, FDIC, FTC, SEC, and CFTC) apply to the financial institutions within each agency’s respective jurisdiction.\textsuperscript{1369}

### 10.2.3.1 Scope

The GLBA imposes disclosure and security requirements for financial institutions with respect to consumers’ NPI. ‘Financial institutions’ include any business that engages in financial activity described in section 1843(k) of Title 12, such as “lending, exchanging, transferring, investing for others, or safeguarding money or securities,” providing investment advice, and making a market for securities.\textsuperscript{1370} Thus, the scope of the GLBA extends to a wide variety of financial companies, including banks, bank holding companies, securities firms, credit unions, money transmitters, check cashiers, travel agencies, and real estate brokers.\textsuperscript{1371}

The GLBA also defines nonpublic personal information as “personally identifiable financial information—(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.”\textsuperscript{1372} This encompasses a wide variety of consumer information, including information obtained in loan applications, account balances and transactional histories, the fact that an individual is a customer, information collected through an Internet cookie, and information from a consumer report.\textsuperscript{1373}

NPI, however, excludes publicly available information, meaning “information that [the financial institution has] a reasonable basis to believe is lawfully made available to the general financial activity. 15 U.S.C. §§ 6804(a)(1)(A) - (B), 6805(a)(3)-(5); 7 U.S.C. § 7b-2(a); see also 12 C.F.R. § 1016.1(b)(3).


\textsuperscript{1368} Finalization of Interim Final Rules (Subject to Any Intervening Amendments) Under Consumer Financial Protection Laws, 81 Fed. Reg. 25323 (Apr. 28, 2016); 12 C.F.R. § 1016 et seq.

\textsuperscript{1369} 12 U.S.C. §§ 5481(12)(J), 5514(b)-(c), 5515(b)-(c); 15 U.S.C. §§ 6801(b), 6804(a)(1)(A), 6805.

\textsuperscript{1370} 15 U.S.C. § 6809(3); 12 U.S.C. § 1843(k); 12 C.F.R. § 1016.3(l).


\textsuperscript{1373} 12 C.F.R. § 1016.3(p), (q) (CFPB); 16 C.F.R. § 313.3(n), (o) (FTC); 17 C.F.R. § 160.3(u), (v) (CFTC); 17 C.F.R. § 248.3(t), (u) (SEC).
public from: (i) Federal, state, or local government records; (ii) Widely distributed media; or (iii) Disclosures to the general public that are required to be made by Federal, state, or local law.”

The GLBA distinguishes between consumers and customers, providing only limited protections for consumers. Here, the term ‘consumer’ means “an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.”

A ‘customer,’ by contrast, is a consumer who has a continuing relationship with a financial institution “under which [the financial institution] provide[s] one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.”

As discussed further below, the GLBA requires that consumers be given notice before financial institutions disclose their NPI to third parties, while customers are entitled to such notice at the time they become customers and every year thereafter. Additionally, the GLBA’s information safeguard provisions apply to the NPI of customers only, not of consumers.

10.2.3.2 Requirements

The GLBA generally prohibits a financial institution from disclosing NPI to a nonaffiliated third-party unless the financial institution provides notice to its customers and consumers about its privacy policies and practices, and gives the consumers an opportunity to opt out. The CFPB requires this notice to be clear and conspicuous. An initial notice must be given to a customer

1374 12 C.F.R. § 1016.3(r)(3(ii) (“Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper, or a Web site that is available to the general public on an unrestricted basis. A Web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public”).

1375 12 C.F.R. § 1016.3(r)(1).


1377 16 C.F.R. § 313.3(h), (i) (FTC); 17 C.F.R. § 160.3(k), (l) (CFTC); 17 C.F.R. § 248.3(j), (k) (SEC); see also 12 C.F.R. pt. 30(I)(C)(2)(d), (e) (OCC).


1379 15 U.S.C. § 6802. (“A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless—(A) such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 6804 of this title, that such information may be disclosed to such third party; (B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and (C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.”).

no later than when the customer relationship is established, and to a consumer before disclosure of
the NPI to a nonaffiliated third-party.\footnote{1381} An annual notice must also be given to a customer at
least once every twelve months during the course of the customer’s relationship with the financial
institution.\footnote{1382}

The notice must detail certain information: the categories of NPI being collected and the
information that may be disclosed; categories of affiliates and nonaffiliates with whom the NPI is
shared; the financial institution’s confidentiality and security policies; and information concerning
how the consumer may opt out of the financial institution’s disclosure with nonaffiliated third
parties.\footnote{1383} Notice must be given so that each consumer “can reasonably be expected to receive
actual notice in writing or, if the consumer agrees, electronically.”\footnote{1384} Thus, for example, if notice
and reasonable opportunity to opt out is given, a financial institution may disclose a consumer’s
NPI – but not account number – to an unaffiliated third-party for marketing purposes.\footnote{1385}

The GLBA also requires financial institutions to protect the security and confidentiality of
customers’ nonpublic personal information, and authorizes federal regulators to establish
information safeguard standards: “(1) to insure the security and confidentiality of customer records
and information; (2) to protect against any anticipated threats or hazards to the security or integrity
of such records; and (3) to protect against unauthorized access to or use of such records or
information which could result in substantial harm or inconvenience to any customer.”\footnote{1386}

The Safeguard Rules, which implement sections 501(b) of the GLBA (15 U.S.C. § 6801),
set forth standards for developing and implementing administrative, technical, and physical
safeguards to protect the security, confidentiality, and integrity of customer information.\footnote{1387} Some
agencies require specific elements for an information security program. For example, the FTC
requires financial institutions to maintain a security program that designates an employee to
coordinate the security program, identifies reasonably foreseeable risks, designs and implements
information safeguards to control the risks, oversees service providers (i.e., a person or entity that

\footnote{1381} 12 C.F.R. § 1016.4(a).
\footnote{1382} 12 C.F.R. § 1016.5(a).
\footnote{1383} 12 C.F.R. §§ 1016.6, 1016.7.
\footnote{1384} 12 C.F.R. § 1016.9 (explaining that reasonable expectation of actual notice may include hand
delivery, mail to last known address, and posting on an electronic site requiring consumer
acknowledgment of receipt if the consumer transacts electronically).
\footnote{1385} 12 C.F.R. §§ 1016.10, 1016.12. The GLBA does not prohibit disclosure of NPI to an affiliate
— i.e., “any company that controls, is controlled by, or is under common control with another
company.” See 15 U.S.C. §§ 6802(a); 6809(6).
(FDIC); 12 C.F.R. pt. 748 app. A (NCUA); 16 C.F.R. pt. 314 (FTC); 17 C.F.R. § 160.30
(CFTC); 17 C.F.R. § 248.30 (SEC).
has access to customer information in the course of providing a service to the financial institution, conducts tests, and adjusts accordingly.\textsuperscript{1388}

10.2.3.3 Penalties

There is no private right of action for violations of the GLBA,\textsuperscript{1389} because the statute provides enforcement authority to federal agencies.\textsuperscript{1390} For example, the CFPB is authorized to issue cease and desist orders,\textsuperscript{1391} and to commence civil actions for civil penalties (which can range from $5,000 to $1,000,000 per day depending on whether the financial institution violated the law recklessly or knowingly) or legal and equitable relief\textsuperscript{1392} for violation of the privacy provisions of the GLBA.

10.2.3.4 Application to Blockchain Businesses

There has not been any litigation or enforcement activity seeking to apply the GLBA to blockchain or virtual currency companies. In light of the GLBA’s statutory definitions, however, certain virtual currency and blockchain technology companies are, or conceivably could be, covered by the GLBA. For example, the description of financial activity under the Bank Holding Company Act of 1956, to which the GLBA’s definition of “financial institution” refers, includes dealing in or making a market in securities.\textsuperscript{1393} Thus, virtual currency exchange sites that allow the trading of ICO tokens – which could be securities, according to the SEC\textsuperscript{1394} – might well be considered financial institutions for GLBA purposes. Virtual currency exchanges sites that accept fiat currency could also fall within the scope of GLBA since the Bank Holding Company Act also includes transferring money as a financial activity.\textsuperscript{1395}

Additionally, as lending money is also considered a financial activity,\textsuperscript{1396} several blockchain DApps that provide loans, such as SALT Lending,\textsuperscript{1397} which allows consumers to obtain cash loans by staking their virtual currencies as collateral, would have to comply with the GLBA.

Thus, blockchain technology companies falling within the ambit of the GLBA must provide notice to consumers and safeguard their customers’ NPI. A blockchain technology

\begin{thebibliography}{99}
  \bibitem{1388} 16 C.F.R. § 314.4.
  \bibitem{1390} \textit{Id}.
  \bibitem{1391} 12 U.S.C. § 5563.
  \bibitem{1392} 12 U.S.C. §§ 5564, 5565.
  \bibitem{1394} \textit{See} Chapter 8 (Securities Regulations).
\end{thebibliography}
company would likely not have to provide notice of the company’s privacy policies and practices and opt-out procedures in connection to the disclosure of information recorded on a public blockchain, where access is available to the general public, as opposed to a private blockchain, which is restricted to certain individuals. However, if the business collects non-public information from consumers, it may need to provide them with notice and the opportunity to opt out. Also, since blockchain transactions are electronic, notice may be posted on the company’s website or DApp platform.\footnote{1398}{12 C.F.R. § 1016.9(a) - (b).} The company, however, must receive the consumer’s acknowledgment as a necessary step before providing the financial product or service.

Finally, blockchain technology companies must secure their customers’ NPI. If the information is stored on a blockchain, the company should assess various risks,\footnote{1399}{See Chapter 3 (Threats to Blockchain Networks).} such as that of a 51% attack or distributed denial-of-service, and adjust its security program accordingly.
Chapter 11

11 Property

11.1 Blockchain for Title Registry

Despite the prevalence of real estate transactions and the critical importance for government agencies to maintain ownership and lien records that are accurate and current, such records are generally maintained in an inefficient and costly manner that exposes them to risk of human error and natural disasters. These issues exist worldwide. For example, land disputes remain prevalent in Haiti because all of the country’s land records, which were stored solely on paper, were destroyed in the 2010 earthquake.1400 Similarly, disputes exist over land in the Gaza Strip because the West Bank has been under Ottoman, British, Jordanian, and Israeli control within the last century, which has often resulted in a complicated land registry and uncertain titles.1401 Using a blockchain as an immutable digital record of title registry would remedy such deficiencies in the existing land recording systems.1402

Further, much of the real property purchase and recordation process is not transparent to either the public or financial stakeholders. Blockchain technology has the ability to solve many of these issues as it can verify records of transactions for digital files. These records are uniquely identifiable by their hash key on a block in the immutable chain of blocks on the distributed ledger.1403 Once written to the blockchain, these transactions cannot be altered accidentally or fraudulently.1404 Through the use of hashes on a public blockchain to document every real estate transaction in a particular jurisdiction, common real estate issues, such as determining the true legal owner of a piece of real property, could be resolved much more easily and quickly.

Additionally, blockchain technology would provide cost savings. For example, in the United States, many county recorders spend an inordinate amount of time trying to locate records for so-called “nuisance” properties—i.e., those subject to tax liens, abandonment, adverse possession, and other title issues—which are likely targets for land title fraud.1405 A digital registry with all records hashed onto a public blockchain would generally eliminate this wasteful burden.1406

---


1403 See generally Chapter 2 (Blockchain Technology), supra.

1404 Id.

1405 Reese, supra note 1402.

1406 Id.
Blockchain technology could also be used to create a public registry of mortgages and deeds of trust, as well as assignments of those documents. One of the main problems during the mortgage crisis was the inability of financial institutions to prove they were the holders of the mortgages and deeds of trust for the properties they were foreclosing upon. Blockchain technology offers a framework for a system of clear, immutable records of mortgage and deed of trust ownership.

11.1.1 Blockchain Technology Can Obviate the Need for Title Insurance in the U.S.

The transparency, low cost of maintenance, low administrative burden, and resilience to fraud makes blockchain technology an appealing solution to land registry issues. The distributed ledger component of blockchain technology makes it ideal for registries. In the real estate context, Executable Distributed Code Contracts (EDCCs) could readily be used to effectuate land transfers. The terms of the sale and transfer of the property could be programmed into an EDCC, which could also automatically register the new owner’s deed with the local recorder and send out notification of that recordation to all interested parties.

Unlike land registration authorities in many other countries, county recorders in the United States do not guarantee that a recorded title is indefeasible. To protect against challenges to title, therefore, real estate purchasers obtain costly title insurance. If all records existed on a public blockchain, however, an EDCC for the sale of real estate could readily be written to ensure that the title could only pass from seller to buyer if there were no defects in the chain of title. If all property ownership records were maintained on a public blockchain, and all property transfers had to be conducted on that same blockchain, title insurance would be unnecessary.

---


1409 See generally Chapter 2 (Blockchain Technology).

1410 See generally Chapter 16 (EDCCs).

1411 Id.


11.1.1.1 Accenture’s Editable Blockchain

Government officials have signalled their awareness that incorrect data could potentially be stored forever on the immutable blockchain. As the Vermont legislature put it, “blockchain technology offers no assistance in terms of the reliability or accuracy of the records contained in the blockchain; if bad data is used as an input, as long as the correct protocols are utilized, it will be accepted by the network and added to the blockchain.”\(^{1414}\) U.S. regulators are particularly sensitive to these issues as privacy legislation provides consumers with a right to correct their data, also known in Europe as the “right to be forgotten,” which is at odds with the concept of an immutable ledger.\(^{1415}\)

To address these issues, Accenture has developed and patented\(^ {1416}\) an “editable” blockchain, which allows a central administrator to edit or delete incorrect or fraudulent information stored on a permissioned blockchain.\(^ {1417}\) Unlike a public blockchain, a permissioned blockchain requires permission to read the information contained on the ledger, and the parties who can transact on the chain are limited to a private class.\(^ {1418}\) The data on Accenture’s permissioned blockchain can only be edited under “extraordinary circumstances”\(^ {1419}\) through the use of a new function named “chameleon,” which recreates algorithms that link blocks together with private keys, thereby allowing administrators to edit, rewrite, and remove blocks of information.\(^ {1420}\)

Accenture’s technology would allow for a correctable blockchain-based land registry, which would be useful for several reasons. First, it can alleviate stress with respect to data storage. Presently, blockchain transaction volumes are relatively low. If utilized for a major project, however, like a land registry for a large geographic region, storing all data on a public blockchain would require a massive on-chain data scale. An editable, permissioned blockchain would allow


\(^{1417}\) Accenture, \textit{supra} note 1416.


\(^{1420}\) \textit{Id.}
for hard and soft forks to alleviate some system storage stress – e.g., by removing aging transaction data that is no longer relevant to the determination of the land title.1421

Second, illegal and fraudulent transactions can stand uncorrected on an immutable blockchain. In the case of the $60 million hack of The DAO, the Ethereum miners succeeded in building a consensus to roll back transactions by creating a hard fork.1422 This was a drastic measure that many in the Ethereum community opposed, but it ultimately resulted in the return of consumer funds.1423

Where a hacker manages to conduct a fraudulent transaction to obtain title to a particular piece of property – e.g., by subverting identity verification procedures – there is no similarly compelling reason for the mining community to get involved. Indeed, when Parity recently lost about $160 million in Ether as the result of a security exploit,1424 the Ethereum community opted not to hard fork to save the lost Ether, because Ethereum developers warned that doing so could change an important invariant of the Ethereum Virtual Machine, leading to unexpected bugs and flaws throughout the blockchain.1425 As such, corrections on the individual level would be difficult, if not impossible, to implement without an editable blockchain.1426

Third, human error will ultimately cause transaction booking errors on an immutable blockchain because the risk of human error can never be truly eliminated. If a human error is not harmless, and a transaction needs to be reversed, doing so is impossible on a public blockchain.1427

Finally, the mandates of many countries’ privacy laws are incompatible with a public, immutable blockchain. For example, the right to erasure directives under the European Union General Data Protection Regulation,1428 and the U.S. Gramm-Leach-Bliley1429 and Fair Credit Reporting Acts,1430 give all consumers the right to withdraw or redact their data in certain circumstances, which is impossible on an immutable platform. Immutability is one of the major

---


1423 Id.


1426 Treat, supra note 1421.

1427 Id.


regulatory concerns hindering wide-scale adoption of blockchain technology. But permissioned systems, which combine distributed ledger technology with the ability to make changes through a governance construct that users can trust and audit may be a basis for “pragmatic immutability.”

Unsurprisingly, some observers have criticized the concept of an editable blockchain, questioning why a distributed blockchain database would be used at all if the tamper-resistant characteristics were removed. Without the immutability of the blockchain, they argue, a digital land registry would suffer from many of the same defects as the current system.

11.1.2 International Efforts to Implement Blockchain Land Registries

11.1.2.1 Sweden

In 1970, the Lantmäteriet (i.e., the Swedish Mapping, Cadastre, and Land Registration Authority) undertook the task of digitizing the country’s land registry. Only the records for newer properties were digitized, however, and many older property title deeds had been lost. Recently, several companies and government agencies, such as Kairos Future, Lantmäteriet, Landshypotek Bank, SBAB, Telia, and ChromaWay, have implemented a land registry blockchain test platform in Sweden to study the possibility of using blockchain technology for land registry as well as mortgage transactions and records. The development group conducted its first project in June 2016, and concluded a second project to further test and develop the blockchain solution in March 2017.

The testbed implemented a private blockchain that can be run by a group of public or private entities through a software application running EDCCs tailored to the conditions of authorization for contracts and mortgage deeds. The resulting report, based on the experience with the testbed, suggested a secure process for real estate transactions with the following characteristics:

1) All involved actors will have a digital file representing the agreement of ownership of the real estate, mortgage deeds and the transaction process. These files can be stored in the cloud, locally, or by some other method of the actor’s choosing.

---

1431 Treat, supra note 1421.
1434 Id. at 72.
1435 Id.
1436 Id. at 3.
2) The authenticity of the process, signatures, file confirming ownership, mortgage deeds, etc. will be secured with a blockchain. The Swedish Lantmäteriet will store the blockchain with the proofs, but the blockchain will also be stored and validated by other actors. Thus, authorized third parties could verify information easily. These third parties would usually be actors who are part of the process, e.g., banks, buyers, sellers, and real estate agents.

3) Records and files that should be public according to Swedish law will be public, and those that should be confidential will stay confidential.

4) No bearer instrument will be stored on the blockchain. This precludes the risk of such authoritative documents being lost, stolen, or tampered with. Bearer instruments could be implemented in the future, but it should be noted that doing so entails risks and legislative uncertainties that require further investigation.

5) The only way to steal a property is by entering a new real estate transaction process with stolen or forged identification. The security of the ID solution can be improved according to the requirements of the system in question. More stringent identification procedures (e.g., photos of physical ID cards, biometric identification, multi signatures) can easily be implemented.

6) The current process is designed to involve Lantmäteriet, real estate agents, buyers, sellers, and banks. These are the parties involved in most real estate transactions in Sweden. The process can be redesigned to involve other actors such as notaries, insurance companies and local public authorities.

The report concludes that the value of such a land registry blockchain would be substantial for countries like Sweden, which currently lack a trustworthy real estate ownership record and land registry. The testbed provided reliable proof that it is easier to operate, more cost-effective, and a faster way to increase GDP in the medium term than current real estate transaction processes. Kairos Future predicts that “it will serve as a foundation for better investments in land, enable the development of a mortgage market and a credit market in general, and become an institution for trust in one of the most fundamental parts of an economy: land and real estate.”

In March 2018, Lantmäteriet announced that it would be conducting its first property transaction on the blockchain platform and was shortlisting volunteers to participate in buying and selling property on the blockchain system.

11.1.2.2 Russia

---

1437 *Id.* at 4-5.
1438 *Id.* at 5.
1439 *Id.*
1440 *Id.*
In October 2017, the Ministry of Economic Development of the Russian Federation announced its plans to conduct a pilot program to test the reliability of using blockchain to track real estate information.\footnote{Press Release, \textit{A Pilot Blockchain Project will be Held in Moscow on the Basis of Rosreestr}, Ministry of Economic Development of the Russian Federation (Oct. 18, 2017), \url{http://economy.gov.ru/minec/press/news/2017181003}; see also Jeremy Nation, \textit{Russia’s Ministry of Economic Development to Test Blockchain Land Registry}, ETHNews (Oct. 20, 2017), \url{https://www.ethnews.com/russias-ministry-of-economic-development-to-test-blockchain-land-registry}.} The announcement indicated that the pilot program “will be aimed at increasing the availability of information on the property registry, guarantees of protection of property rights, as well as the level of citizens’ trust in the sphere of turnover of real estate.”\footnote{Ministry of Economic Development of the Russian Federation, \textit{supra} note 1442.}

In March 2018, Rosreestr, the Russian federal body responsible for state registration of real estate, announced that it would also be conducting two pilot programs to determine whether blockchain technology can improve Russia’s real estate system.\footnote{Fernando Curvecis, \textit{Rosreestr Wants To Spend Two Experiments on the Introduction of Blockchain Technology}, Take Coins (Mar. 23, 2018) \url{https://takecoins.tk/cryptocurrency/rosreestr-wants-to-spend-two-experiments-on-the-introduction-of-blockchain-technology/}.} The first program is similar to the Ministry of Economic Development’s announcement, and will focus on the creation of a blockchain registry of real property rights on the Ethereum blockchain.\footnote{Id.} The second is premised on the automation of the process of examining legal real estate documents through EDCCs.\footnote{Id.} Rosreestr hopes to complete both projects by December 2018.\footnote{Id.} Thereafter, Rosreestr will assess the feasibility of the technology and draft corresponding legislative changes.\footnote{Id.}

11.1.2.3 Georgia

In 2016, the Georgian government joined with the bitcoin software firm Bitfury Group in launching a project to register land titles through a private blockchain, with a verification follow-up to occur on bitcoin’s public blockchain. After testing the software on a few dozen land title registrations, the Georgian National Agency of Public Registry became the first national government to use the bitcoin blockchain to secure and validate official actions.\footnote{Laura Shin, \textit{The First Government to Secure Land Titles on the Bitcoin Blockchain Expands Projects}, Forbes (Feb. 7, 2017), \url{https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#296bf2e4dcde}.} In February of 2017, the Republic of Georgia committed to using the bitcoin network to validate property-related government transactions.\footnote{Id.}
11.1.2.4 Ghana

In May of 2017, blockchain start-up BenBen announced that it would be building a land registry in Ghana to help secure property rights for citizens. The idea came to fruition when the start-up’s founders, Daniel Block and Emmanuel Noah, attended an event at the University of Kenya, where they became aware of the massive land rights issues endemic to much of Africa.

In Ghana, land records are currently stored only on paper, which become lost and destroyed over time, causing inconsistencies among stakeholders. Even where the title deeds are located, the degree of fraud is so high that the paper registry system is unenforceable in the Ghana court system, meaning that collateralization of property rights there is virtually impossible. Due to the unenforceability of the paper registrations, banks will not accept land as collateral, which leaves millions without the option of leveraging property for loans or relying on the rule of law for protection.

BenBen is creating a top-of-stack land registry and verification platform for use by financial institutions, which will capture all property transactions and verify the data. The start-up plans to work with financial institutions to update current registries, enable EDCC transactions, and distribute private keys for clients to help ensure trusted transactions between all parties.

11.2 EDCCs for Real Estate Transactions

In October of 2017, Ethereum-based start-up Propy announced the first real estate transaction to be completed on a blockchain in Kiev, Ukraine. The properties were exchanged P2P through EDCCs that played the roles of attorney and escrow agent. Instead of a title company or notary, the EDCC acted as an escrow agent and held funds in a secured decentralized...


1452 Id.


1454 Id.

1455 Id.

1456 Id.

1457 Id.


1459 Id.
and verified hash.1460 Once the conditions of the EDCC had been executed, the funds were transferred to the seller and the escrow function of the EDCC prevented “double-spending” to ensure that the same property could not be sold by the same person more than once.1461

One major benefit of using the EDCC as an alternative to an escrow agent, according to Propy, is that the government will no longer need to trust vulnerable traditional databases and can collect any property tax automatically from the EDCC instead of from notaries or escrow companies.1462 Propy’s application secures the funds for a transaction with two private keys:

1) A transacting key (held by the seller), registered in advance with the Propy Identity Service to ensure verification of identity, can be used to execute the Deed EDCC, which will eventually be tailored to the requirements of real estate transfers in each country to ensure compliance with local regulations.1463 During the login operation, the key is imported via the EDCC into the Propy Transaction Platform. Propy performs ownership verification and generates a preliminary agreement, which is signed electronically by the seller, buyer, and broker. The deed EDCC then changes the property state to “Pending.”1464

2) An asset transfer key (held by the buyer) is registered with the Deed EDCC, which then accepts Ether from buyer’s asset wallet only and releases Ether to the seller’s asset wallet only.1465 After payment, the notary verifies the property ownership and transfer conditions in the Registry of Ownerships and Burdenings of Ukraine. The Deed EDCC then changes the status of the transaction to “Approved,” and a registry fee in Propy tokens is automatically transferred from the buyer’s wallet.1466

Both keys are private such that Propy cannot access them.1467

1460 Id.
1461 Id.
1464 Id.
1465 Id.
1466 Id.
1467 Id.
In March 2018, Propy partnered with the Vermont government to use Propy’s blockchain registry software to create EDCCs for both property contracts and deed contracts.\footnote{Alexander Voloshyn, First Government Sanctioned Blockchain Recorded Real Estate Deal in the US, Propy (Mar. 21, 2018) https://blog.propy.com/first-government-sanctioned-blockchain-recorded-real-estate-deal-in-the-us-bb83e8292a7f.} With Propy’s software, the parties to the real estate transaction first prepare a property EDCC, which is created once for the property and is applicable to all sales or transfers involving that property moving forward, so long as the property EDCC remains in the registry.\footnote{Id.} Next, to allow for the inspection of the historical data associated with the property, a deed EDCC is prepared for each transaction associated with the property.\footnote{Id.} Then, the conveyance data along with the hash of the recorded deed is written into the deed EDCC as a separate transaction.\footnote{Id.} Finally, the deed EDCC is registered into the Propy registry and the registration fee is paid in PRO tokens.\footnote{Id.} Propy’s next step in Vermont is to collect feedback from the recorder’s office and implement a user interface that simplifies the Propy registry for use by the government.\footnote{Id.}

In November 2017, Ireland-based start-up Confideal introduced its Ethereum-based real estate DApp, which is powered by a pre-programmed EDCC to execute the property transfer in conjunction with an EDCC constructor application. The user-friendly constructor application allows buyers and sellers to explicitly set the terms of a transaction through customizable EDCCs, which play the role of an impartial escrow agent.\footnote{CryptoNinjas, Blockchain Escrow App Confideal Announces Launch of Smart Contract Constructor (Sept. 19, 2017), https://www.cryptoninjas.net/2017/09/19/blockchain-escrow-app-confideal-announces-launch-smart-contract-constructor/.} Where a dispute occurs about the execution of a transaction and the parties cannot reach a resolution, Confideal allows them to request the advice of a qualified arbitrator within the platform who will anonymously arbitrate and resolve the dispute. The platform aims to solve the problem of costly and inefficient international property disputes by working on a trustless basis.\footnote{Id.}
Chapter 12
12 Data Management and Protections

12.1 Privacy Protections


One reason the United States has not developed a single, unified federal data protection law is that government policy has traditionally deferred to the private sector. Companies implement their own policies and develop their own technologies, forcing individuals to self-regulate the dissemination of their private data. The Federal Trade Commission (FTC), which has broad authority to “investigate unfair and deceptive acts and practices in or affecting commerce,”\footnote{Fed. Trade Comm’n, Start with Security: A Guide for Business (Jun. 2015), \url{https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf}.} has increasingly used this authority to fill the legislative gap and provide advice for companies on how to protect consumer data.

More specifically, the FTC has provided guidance concerning: (1) the general security of personal information, (2) how to sensibly control access to data, (3) requirements for secure passwords and authentication, (4) secure storage of sensitive personal information, (5) segmenting and monitoring networks, (6) providing secure remote access to networks, (7) applying sound security practices when developing new products, (8) ensuring that service providers implement reasonable security measures, (9) procedures for keeping security current and addressing vulnerabilities, and (10) securing paper records, physical media, and devices.\footnote{Fed. Trade Comm’n, Start with Security: A Guide for Business (Jun. 2015), \url{https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf}.}

In many commercial data scenarios, blockchain technology enables companies to implement comprehensive solutions for complying with the FTC’s guidance. Notably, distributed ledgers allow transactions to occur without either of the parties directly disclosing their...
identities.\textsuperscript{1483} This anonymity, or pseudonymity, means that transactions cannot be traced back to individual parties, thereby preserving the fundamental right to self-determination.\textsuperscript{1484}

\textbf{12.1.1 Relevant Federal Laws}

\textbf{12.1.1.1 The Wiretap & Electronic Communications Privacy Act}

The Wiretap Act was first passed as Title III of the Omnibus Crime Control and Safe Street Acts of 1968 to regulate the collection of the actual content of wire and oral communications.\textsuperscript{1485} In 1986, the Act was extended by the Electronic Communications and Privacy Act (ECPA) to cover all electronic communications.\textsuperscript{1486}

The Wiretap Act prohibits the intentional interception, use, and disclosure of wire and electronic communications by third parties, including the government.\textsuperscript{1487} The Act effectively prohibits the wiretapping of telephones and the installation of electronic devices that read Internet traffic. Section 2510(1) defines a “wire communication” as:

any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.\textsuperscript{1488}

An “aural transfer” is defined as “containing the human voice at any point between and including the point of origin and point of reception.”\textsuperscript{1489} If there is no genuine human voice, either alone or in a group conversation, then the communication cannot be deemed a wire communication for the purposes of the Wiretap Act.\textsuperscript{1490}

Other portions of the law apply to non-voice communications. Section 2510(2) defines an “electronic communication” as:

\begin{itemize}
  \item \textsuperscript{1484} Stefan Wilke, Blockchain from a Perspective of Data Protection Law, Deloitte https://www2.deloitte.com/dl/en/pages/legal/articles/blockchain-datenschutzrecht.html# (last visited Nov. 10, 2018).
  \item \textsuperscript{1485} 18 U.S.C. §§ 2510-2522.
  \item \textsuperscript{1486} Id.
  \item \textsuperscript{1487} 18 U.S.C. § 2511(1).
  \item \textsuperscript{1488} 18 U.S.C. § 2510(1).
  \item \textsuperscript{1489} 18 U.S.C. § 2510(18).
  \item \textsuperscript{1490} United States v. Torres, 751 F.2d 875, 885-86 (7th Cir. 1984) (holding that “silent television surveillance” cannot be considered a wire communication under Title III because no aural acquisition occurs).
\end{itemize}
any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;
(B) any communication made through a tone-only paging device;
(C) any communication from a tracking device (as defined in section 3117 of this title); or
(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.1491

As clarified by the 1986 House of Representatives Report, “as a rule, a communication is an electronic communication if it is neither carried by sound waves nor can fairly be characterized as one containing the human voice.”1492

In United States v. Councilman,1493 the First Circuit upheld Wiretap Act charges against a defendant bookseller who also provided an email service for his clients. The defendant was accused of secretly copying emails to his clients from competitor Amazon.com and sending the copies to his own personal account. A panel initially ruled the emails were not “intercepted” within the meaning of the law because they were in temporary storage on a computer system, not “in transit,” at the time that the copying and sending took place.1494 After rehearing the case en banc, however, the First Circuit reversed, holding that the term “electronic communication” includes transient electronic storage because that step is intrinsic to the communication process.1495

Section 18 U.S.C. §2510(4) defines “interception” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” In United States v. Ropp,1496 the district court held that the use of a key logger to intercept keyboard strokes does not violate the Wiretap Act because the transmission at issue did not fall within the meaning of “electronic communications.”1497 The court reasoned that the law requires transmissions be made “in interstate commerce,” and there was no active Internet connection when the key logger was active.1498 Similarly, in United States v. Scarfo,1499 the district court held that a key logger device on a personal computer does not intercept

---

1493 United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (en banc).
1494 United States v. Councilman, 373 F.3d 197, 201 (1st Cir.2004).
1495 Councilman, 418 F.3d at 79.
1497 Id. at 837.
1498 Id.
communications if it is configured so that keystrokes are not recorded when the computer’s modem is in use.\textsuperscript{1500}

Individuals who violate the Wiretap Act can be fined and sentenced to as much as five years in prison.\textsuperscript{1501} Further, victims are entitled to bring civil suits to recover actual damages, punitive damages, and attorney’s fees.\textsuperscript{1502}

There are three major exceptions to the prohibitions in the Wiretap Act and ECPA. First, the ECPA has a law enforcement exception that has been interpreted to allow federal agents to obtain and review six-month-old electronic communications, provided there is a subpoena.\textsuperscript{1503} Civil liberties advocates have criticized the fact that only a subpoena is required, not a warrant approved by a judge, arguing that the Act’s language gives federal agents too much power.\textsuperscript{1504}

Second, Section 2511(2)(a)(i) of the Wiretap Act permits communications service providers\textsuperscript{1505} “to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service,” with certain limitations.\textsuperscript{1506} This exception gives such providers the limited\textsuperscript{1507} right to “to intercept and monitor [communications] placed over their facilities in order to combat fraud and theft of service.”\textsuperscript{1508} The limited exception allows providers to conduct reasonable monitoring that balances the protection of the providers’ rights and property against their subscribers’ right to privacy.\textsuperscript{1509}

\begin{footnotesize}
\begin{enumerate}
\item Id. at 581-582.
\item 18 U.S.C. § 2511(4)(a).
\item 18 U.S.C. § 2520.
\item 18 U.S.C. § 2520.
\item That is, “an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication...” 18 U.S.C. § 2511(2)(a)(i).
\item Specifically, “a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.” Id.
\item \textit{United States v. Auler}, 539 F.2d 642, 646 (7th Cir. 1976) (“This authority of the telephone company to intercept and disclose wire communications is not unlimited.”).
\item \textit{United States v. Harvey}, 540 F.2d 1345, 1351 (8th Cir. 1976) (“The federal courts ... have construed the statute to impose a standard of reasonableness upon the investigating communication carrier.”).
\end{enumerate}
\end{footnotesize}
Finally, Section 2511(2)(g)(i) of the Wiretap Act permits any individual to intercept electronic communications made through a system “that is configured so that such electronic communication is readily accessible to the public.”\(^{1510}\) Thus, any information transmitted or transacted on a public blockchain, such as Ethereum or bitcoin, would be fair game for interception under the Act. However, there is no practical method of “intercepting” a transaction on a public blockchain. Regardless, transactions on a public blockchain can be verified at any time by any user, including government agencies, so the wallet addresses and transaction hashes are visible without any interception of communications required. The same is not true of private blockchains, which do not publicly list their transactions and thus, under the Wiretap Act, can only be accessed by a “provider” or, for transactions older than six months, a federal agent with a subpoena.\(^{1511}\)

**12.1.1.2 The Privacy Act**

The Privacy Act of 1974 was enacted to safeguard individuals from the misuse of federal government records, to provide individuals with the right to access records concerning them that are maintained by federal agencies, and to establish a Privacy Protection Study Commission.\(^{1512}\)

The Privacy Act requires that federal agencies publicly identify all of their record systems in the Federal Register.\(^{1513}\) It mandates that “no agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.”\(^{1514}\) Federal officials handling personal data are “bound by the Privacy Act not to disclose any personal information and to take certain precautions to keep personal information confidential.”\(^{1515}\) As defined by the law’s guidelines, a “disclosure” can be any means of communication, written, oral, electronic, or mechanical.\(^{1516}\)

In interpreting the Privacy Act, several Circuits have held that a “disclosure” does not occur if the communication is made to someone already aware of the disclosed information.\(^{1517}\) The D.C. Circuit, however, has taken a more expansive approach. In *Pilon v. United States Department of Justice*, the court of appeals held that the Justice Department’s transmission of a protected record to a former agency employee constituted a disclosure under the Privacy Act even though the recipient had “come into contact with the record in the course of his duties” while employed for the agency.\(^{1518}\) The court reviewed the law’s purpose and legislative history to conclude that

---

\(^{1510}\) 18 U.S.C. § 2511((2)(g)(i).


\(^{1512}\) 5 U.S.C. § 552a(e)(4).

\(^{1513}\) 5 U.S.C. § 552a(e)(4).

\(^{1514}\) 5 U.S.C. § 552a(b).


\(^{1517}\) *See, e.g.*, *Quinn v. Stone*, 978 F.2d 126, 134 (3d Cir.1992); *Kline v. HHS*, 927 F.2d 522, 524 (10th Cir.1991).

Congress intended the term “disclose” to “apply in virtually all instances to an agency’s unauthorized transmission of a protected record, regardless of the recipient’s prior familiarity with it.”

If a Federal agency desires to disclose any records concerning an individual to a third-party, it generally must obtain consent. But there are twelve types of disclosures where the rule does not apply: (1) as required within the agency itself; (2) in response to requests under §552 of the title; (3) for routine uses; (4) to the Bureau of the Census; (5) for statistical research purposes; (6) to the National Archives; (7) in response to law enforcement requests; (8) for the health or safety of an individual; (9) to Congress; (10) to the General Accounting Office; (11) in response to a court order; and (12) under the Debt Collection Act.

Section 552a(i)(1) of the Privacy Act makes unauthorized disclosures a misdemeanor and sets a fine of up to $5,000 for violations. The same penalties apply for maintaining a system of records that fail to comply with the law’s notice requirements. The Privacy Act further permits individuals to file civil actions against agencies, authorizing injunctive relief or monetary damages, depending on the nature of the violation.

---

1519 Id. at 1124.
1520 5 U.S.C. § 552a(b).
1521 5 U.S.C. § 552a(b)(1).
1522 5 U.S.C. § 552a(b)(2).
1523 5 U.S.C. § 552a(b)(3); see also U.S. Dep’t of Justice, Overview of the Privacy Act of 1974, https://www.justice.gov/opcl/conditions-disclosure-third-parties#routine (last visited Nov. 10, 2018) (“[T]he routine use exception, because of its potential breadth, is one of the most controversial provisions in the act…the trend in recent cases is toward a narrower construction of the exception.”).
1525 5 U.S.C. § 552a(b)(5).
1526 5 U.S.C. § 552a(b)(6).
1528 5 U.S.C. § 552a(b)(8).
1529 5 U.S.C. § 552a(b)(9).
1530 5 U.S.C. § 552a(b)(10).
1531 5 U.S.C. § 552a(b)(11).
1534 5 U.S.C. § 552a(i)(2).
1535 U.S. Dep’t of Justice, supra note 1523.
12.1.1.3 The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) of 1986 amended existing computer fraud law under 18 U.S.C. §1030 to protect computer data from theft and ensure that computer-related crimes are punished. The CFAA was written to increase the scope of computer fraud while limiting federal jurisdiction to cases involving protected computers.

Originally, the CFAA protected classified information on government computers and credit information maintained on financial institution computers. In 1994 and 1996, however, Congress amended the statute to cover all computers used in interstate commerce. In 2001, Congress further broadened the law to include any computer “located outside the United States that is used in a manner that affects interstate or foreign commerce or communication in the United States.” This sweeping language arguably reaches all computers anywhere in the world that are connected to the Internet and interacting with a website or computer operating in the United States.

The CFAA is a broad law that protects computer data by allowing civil causes of action where: (1) information is obtained from a protected computer through unauthorized access; (2) computer passwords have been trafficked and can access a computer; (3) damaging spam mail has been sent; or (4) computer data has been damaged or destroyed. Any company victimized by the theft or destruction of data may seek injunctive relief for the return of the data and to prevent its competitive use. CFAA liability is predicated on someone either exceeding authorized access to a computer, which is defined as “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter,” or using a computer with “unauthorized” access, which is not defined.

Federal courts recognize two categories of unauthorized access: those inherent in agency-principal relationships and those explicitly established by the data’s owner. An example of the former occurred in Shurgard Storage Centers, Inc v. Safeguard Self Storage, Inc., where employees who were about to leave their jobs accessed work computers and emailed trade secrets to their new employer. The district court applied common law rules of agency to conclude that the employees’ right to access their old employer’s computers ended when they acquired adverse interests, meaning the employees “were without authorization” when they allegedly obtained and sent the proprietary information to the defendant via e-mail.

---

1538 Id.
1539 18 U.S.C. § 1030(g).
1542 Id. at 1127.
As for explicit access, in *U.S. Greenfiber v. Brooks*, a former employee removed, without permission, all documents, e-mail files, and software installed on her company computer.1543 The district court ruled the employee’s actions violated the CFAA because they flouted procedures that the company had established expressly to protect the confidentiality of its computer data.1544

In addition to civil causes of action, the CFAA criminalizes any unauthorized access to protected computers affecting interstate commerce.1545 Famously, activist Aaron Swartz was indicted for mass-downloading articles from the journal site JSTOR in violation of CFAA provisions (a)(2), (a)(4), (c)(2)(B)(iii), (a)(5)(b), and (c)(4)(A)(i)(I), (VI).1546 In 2013, the case was dismissed as a result of Swartz’s untimely suicide.1547

While the CFAA protects data and provides civil remedies for companies whose data has been stolen, the criminal provisions have been criticized for making it a crime to violate the terms of service of Internet sites, which can be changed at any time without notifying users.1548 Federal prosecutors present the CFAA as an essential tool for protecting the nation’s computers, but critics view it as an ill-informed and inefficient law that yields disproportionately long sentences relative to the offenses alleged.1549

### 12.1.1.4 The Identity Theft Penalty Enhancement Act

In 2004, due to the substantial increase in identity theft, Congress passed the Identity Theft Penalty Enhancement Act, which created the crime of aggravated identity theft.1550 Section 1028A of the act provides: “whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.”1551 If the violation is connected to terrorist activity, under Section 2332b(g)(5)(B), the punishment is five years’ imprisonment.1552

---


1544 Id.

1545 18 U.S.C. § 1030(c).


1547 See generally Chapter 7 (Cybercrimes).


1549 See generally Chapter 7 (Cybercrimes).


Many blame the extensive use of debit and credit cards, especially online, for the significant upsurge in identity theft. Some have gone so far as to suggest that cyber crime may become the single greatest threat to every person and place in the world within the next five years. Blockchain has been touted as the solution to prevent identity theft from increasing. The key features of this technology – decentralization and cryptography – provide far greater security than debit card PIN numbers, and the blockchain, when coupled with two-factor authentication, is very difficult to hack.

Currently, usernames, passwords, emails, and credit card numbers are all stored on centralized corporate servers, many of which have no authentication requirement at all, and all of which are vulnerable to hacking. Blockchain start-up Civic has created a novel app-based solution that obviates the need for centralized servers. First, Civic collects various bits of identifying information during the app sign-up process. Then it authenticates the information through either a government agency or a third-party identification verification service, depending on the country. Once verification is complete, the app makes a cryptographic hash of the information, inserts the hash onto the blockchain, then erases all personal data from Civic’s servers.

When the Civic user wants to authenticate his or her identity in order to use a third-party’s service, the user provides the identifying information to the service, which then sends the information back through Civic to verify it against the hash on the blockchain. After authentication is verified, the service would ideally delete the user’s information from its servers since it no longer needs that information for identification purposes. Using this model, neither service would ever possess any user information for an extended period of time, such that the risk of cyber-attacks would be substantially diminished.

12.1.1.5 The Children’s Online Privacy Protection Act

Enacted in 1998, the Children’s Online Privacy Protection Act (COPPA) requires the Federal Trade Commission (FTC) to issue and enforce regulations concerning children’s online


1556 Id.

1557 Id.

1558 Civic uses the bitcoin blockchain.


1560 Chester, supra note 1554.
privacy.\textsuperscript{1561} The aim of COPPA is to place parental control over what information can be collected online from children under the age of 13.\textsuperscript{1562}

In 2012, the FTC issued a rule pursuant to COPPA creating new parental notice and consent requirements for organizations that 1) operate a website or online service “directed to children” under 13 that collects personal information from users, or 2) knowingly collect personal information from persons under 13 through a website or online service.\textsuperscript{1563} The new rule revised certain definitions, expanding the circumstances where COPPA applies.\textsuperscript{1564} The definition of “personal information,” for example, now includes not just names and addresses but “online contact information; a screen or user name … persistent identifiers that can be used to recognize a user over time and across different websites; a photograph, video, or audio file containing a child’s image or voice; [and] geolocation information sufficient to identify a street name.”\textsuperscript{1565}

The FTC enforces the rule through complaints by parents, consumer groups or industry members who believe that an operator is violating COPPA.\textsuperscript{1566} A Court can hold violators liable for civil penalties of up to $40,654 per violation.\textsuperscript{1567} The size of the penalty turns on a number of factors: “the egregiousness of the violations, whether the operator has previously violated the Rule, the number of children involved, the amount and type of personal information collected, how the information was used, whether it was shared with third parties, and the size of the company.”\textsuperscript{1568}

The FTC has brought a number of actions against operators, including UMG Recordings, Inc., which was fined $400,000 for COPPA violations in connection with a site promoting 13-year-old pop star Lil’ Romeo.\textsuperscript{1569} In 2006, the owners of the website Xanga were fined $1 million for repeatedly allowing children under 13 to sign up for the service without parental consent.\textsuperscript{1570} At present, age verification is difficult for most websites, and operators cannot tell when children

\textsuperscript{1562} 15 U.S.C. § 6501(a).
\textsuperscript{1564} \textit{Id.}
\textsuperscript{1567} Complying with COPA: Frequently Asked Questions, \textit{supra} note 1565.
\textsuperscript{1568} \textit{Id.}
\textsuperscript{1570} Bob Sullivan, \textit{FTC Fines Xanga for Violating Kid’s Privacy}, NBC News (Sept. 7, 2006), \url{http://www.nbcnews.com/id/14718350/#.WILQ1COZPUI}.
are using the device or login of someone older. To relieve the burden of COPPA compliance, blockchain identity verification services such as Civic could be integrated into the website sign-up processes to ensure that only users with verified ages are allowed to provide personal information.1571

12.1.2 Challenges to Privacy

12.1.2.1 AML/KYC Requirements and PATRIOT Act

Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements are processes used primarily by financial institutions to identify and verify clients.1572 One principal source of AML/KYC requirements is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (PATRIOT Act).1573

The PATRIOT Act’s AML/KYC requirements pose a challenge to data privacy.1574 Banks are required to store a significant amount of personal data that could easily be exploited following a data leak or cyber hack. In July 2017, for example, Italy’s largest bank, UniCredit, was the victim of the largest-ever hacking attack of a European financial institution, which encompassed the theft of data from 400,000 customer accounts.1575 The bank stated that the security breach was due to an “Italian external trade partner,” not internal lapses, and that the breach was immediately blocked upon its discovery. Although the bank had no way to recover the 400,000 lost accounts, it did pledge to upgrade its IT systems in a $2.3 billion project.1576

In September 2017, Equifax, one of the largest credit-reporting companies in the United States, experienced a massive cybersecurity breach that compromised the personal information of 143 million Americans, almost half of the country.1577 Equifax pledged to mail notices to those people whose credit cards or dispute documents had been affected.1578 As one of the largest data breaches ever to date, the event underscores the importance of promulgating new decentralized methods to record, authenticate, and store data.

1571 Chester, supra note 1554.
1572 See generally Chapter 6 (Anti-Money Laundering).
1574 See generally Chapter 6 (Anti-Money Laundering).
1576 Id.
1578 Id.
12.2 Use of Blockchain Technology for Particular Types of Data

12.2.1 Blockchain for Storage of Health Records

A problem facing healthcare systems across the globe is how to share medical data with stakeholders while ensuring data integrity and protecting patient privacy. In the city of Boston alone, for example, 26 different electronic medical records systems are used by hospitals and outpatient treatment centers,1579 each with its own unique language for representing and sharing data.1580 Thus, critical information is spread across many databases and often cannot be accessed when it is most needed.1581 The system is widely viewed as inefficient, and many roadblocks currently hinder the sharing of patients’ health data.

12.2.1.1 HIPAA

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) to improve the portability and continuity of health insurance coverage in group and individual markets. Title II of the Act requires that national standards be established for electronic health care transactions and national identifiers for providers.1582

Section 42 U.S.C. § 1320d-2 sets standards for information transactions and data elements, prescribing that covered entities – i.e., a health plan, clearing house, or health care provider1583 – adopt standards for data that are appropriate for financial and administrative transactions.1584 Covered transactions include (A) health claims, (B) health claim attachments, (C) enrollment and disenrollment in a health plan, (D) eligibility or a health plan, (E) health care payment and remittance advice, (F) health plan premium payments, (G) first report of injury, (H) health claim status, (I) referral certification and authorization, and (J) electronic funds transfers.1585

HIPAA further requires that additional safeguards be established to “(A) ensure the integrity and confidentiality of the information; (B) protect against any reasonably anticipated (i) threats or hazards… (ii) unauthorized uses or disclosures of information; and (C) otherwise to ensure compliance by the officers and employees.”1586 While the safeguards are critical to protect

---


1581 Id.

1582 42 U.S.C. § 1320.


1586 42 U.S.C § 1320d(d)(2).
patient data, each covered entity implements its own safety controls to ensure compliance.\footnote{HIPAA J., \textit{The Benefits of Using Blockchain for Medical Records} (Sept. 26, 2017), \url{https://www.hipaajournal.com/blockchain-medical-records/}.} Under typical circumstances, where each entity uses different safeguards to protect a centralized server that is storing patient data, they are all ultimately vulnerable to data breaches. Blockchain technology is being seriously considered as a decentralized alternative that would allow entities to secure data more efficiently and effectively.

If multiple entities in the healthcare data system support a single blockchain for healthcare records, then none of those entities would need to maintain its own copies of patient data. Instead, a patient could grant any individual provider access to his or her data on the blockchain by providing them with an access key.\footnote{\textit{Id.}} Records of consultations with physicians, x-ray images, blood tests, and prescriptions could all be time-stamped and validated by a trusted entity that has been given an access key. If all healthcare providers committed to the use of one system, medical records would no longer be difficult to piece together, which would reduce costs to patients, because entities under HIPAA are now permitted to charge a fee for providing copies of health data.\footnote{\textit{Id.}} Some progress on these systems is being made. Deloitte’s 2018 Global Blockchain Survey, which polled more than 1,000 executives worldwide, found that 55% of healthcare executives think that blockchain will be disruptive, and more than 60% think they will lose competitive advantage if they fail to get onboard with distributed ledger technology.\footnote{\textit{Id.}} The survey reflects that healthcare executives are particularly interested in certain blockchain features: disintermediation, transparency and accountability, industry collaboration, and new business models.\footnote{\textit{Id.}} Moving forward, 63% of the executives responded that they plan to invest more than one million dollars in blockchain over the next calendar year.\footnote{\textit{Id.}}

MIT Media Lab and Beth Israel Deaconess Medical Center recently conducted a six-month use case trial called MedRec that used a blockchain for the health data exchange between two simulated institutions using two different databases at Beth Israel.\footnote{Ariel Ekblaw \textit{et al.}, \textit{A Case Study for Blockchain in Healthcare: “MedRec” Prototype for Electronic Health Records and Medical Research Data: White Paper} (Aug. 2016), \url{https://www.healthit.gov/sites/default/files/5-56-one_blockchainchallenge_mitwhitepaper.pdf}.} The purpose of the trial was to leverage blockchain properties for MedRec to manage authentication, confidentiality, accountability, and data sharing.\footnote{\textit{Id.}}

\begin{thebibliography}{99}
\bibitem{HIPAA} HIPAA J., \textit{The Benefits of Using Blockchain for Medical Records} (Sept. 26, 2017), \url{https://www.hipaajournal.com/blockchain-medical-records/}.
\bibitem{Id} \textit{Id.}
\bibitem{Id} \textit{Id.}
\bibitem{Id} \textit{Id.}
\bibitem{Id} \textit{Id.}
\bibitem{Id} \textit{Id.}
\bibitem{Id} \textit{Id.}
\bibitem{Id} \textit{Id.}
\end{thebibliography}
Medical stakeholders (e.g., researchers, public health authorities) were incentivized to participate in the network to validate blocks as an alternative to typical transaction mining.\textsuperscript{1595} After participating, the stakeholders received access to aggregate, anonymized data as mining rewards for their efforts to secure the network via Proof-of-Work (PoW).\textsuperscript{1596} In this way, MedRec sought to facilitate the emergence of “data economics,” supplying “big data” to researchers while simultaneously engaging patients and providers in the choice to release metadata.\textsuperscript{1597} The benefits of such a system transcend simply securing data. The sharing of research would allow health care providers to leverage big data in order to analyze the success of various treatments and monitor the spread of diseases in real time.

The trial was considered a success, and plans are underway to expand the pilot, but there are some lingering issues to be resolved. In particular, the MedRec whitepaper does not provide a solution for cases where patient data (e.g., psychotherapy notes) must remain hidden from the patient on the public blockchain. However, even where difficulties have yet to be addressed, the promise of the technology remains clear.

\textbf{12.2.2 Consumer Financial Data}

\textbf{12.2.2.1 Fair Credit Reporting Act}

The Fair Credit Reporting Act of 1970 (FCRA) was enacted primarily to amend the Federal Deposit Insurance Act to require insured banks to maintain certain records, require that certain transactions in U.S. currency be reported to the Department of the Treasury, and provide consumers the right to access their credit data.\textsuperscript{1598} The FCRA was the first data protection law passed in the computer age, and reflected Congress’s concern that “inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system.”\textsuperscript{1599}

The FCRA regulates consumer reporting agencies, users of consumer reports, and furnishers of consumer information. Any institution that willfully fails to comply with any requirement with respect to any consumer is liable to that consumer in an amount equal to the sum of “any actual damages sustained by the consumer as a result of the failure, or damages of not less than $100 and not more than $1,000.”\textsuperscript{1600} Courts may also impose punitive damages, the threat of which is “the primary factor deterring erroneous reporting by the reporting industry.”\textsuperscript{1601}

The FCRA allows credit reporting agencies to share credit data in connection with any credit or insurance transaction so long as the transaction consists of a firm offer of credit or insurance, the reporting agency complies with the exclusion requirements, and the report does not

\footnotesize{\textsuperscript{1595} Id. at 2.  \\
\textsuperscript{1596} Id.  \\
\textsuperscript{1597} Id.  \\
\textsuperscript{1598} 15 U.S.C. § 1681.  \\
\textsuperscript{1599} 15 U.S.C. § 1681(a)(1).  \\
\textsuperscript{1600} 15 U.S.C. § 1681n(a)(1)(A).  \\
\textsuperscript{1601} Brim v. Midland Credit Mgmt. Inc. 795 F.Supp.2d 1255 (N.D. Ala. 2011).}
involve anyone under the age of 21. A consumer may elect to be excluded from any list provided by a consumer reporting agency in connection with a credit or insurance transaction not initiated by that consumer. Otherwise, however, all transactions can be shared without consent to provide relevant information regarding a consumer’s creditworthiness to lenders.

Upon request, every consumer reporting agency (e.g., Equifax, Experian, and TransUnion) must clearly and accurately disclose to the consumer “all information in the consumer’s file at the time of the request” along with “the sources of the information.” The consumer has the right to dispute incomplete or inaccurate information; and, if any information is found to be inaccurate, the agency must correct or delete the data within 30 days.

While blockchain technology promises to make credit reporting more effective and data theft less common, one of its main advantages also presents a major dilemma in the credit reporting context. A cornerstone of blockchain technology is the immutability of the decentralized ledger of transactions. Yet, that same immutability threatens the consumer’s right to erasure of incorrect data. If a blockchain-based record ever required correction, all users on the network would have to agree simultaneously to remove the data. Further, removing one piece of data would alter all subsequent transactions relying on it, thus creating a fork chain and ultimately changing the blockchain’s course.

Start-ups like Bloom Protocol are working on decentralized credit reporting applications. A revised version of the company’s whitepaper states, “[u]sers can review the information before sharing it with the company performing a risk assessment. In the event that the information is incorrect, the user can work with the data vendor to amend their records using the same methods available today. This workflow promotes proactive correction of information before it impacts a user's BloomScore.”

12.2.2.2 The Gramm-Leach-Bliley Act

Congress enacted the Gramm-Leach-Bliley Act of 1999 (GLBA) to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks,

---

sections firms, and other financial service providers.\textsuperscript{1611} This allowed commercial banks, investment banks, securities firms, and insurance companies to consolidate their services.

Sections 6801-6809 of the GLBA create a financial privacy rule that requires financial institutions to provide individual consumers with a privacy notice when the consumer relationship is established, and annually thereafter. Section 6801 requires that financial institutions establish appropriate standards relating to administrative, technical, and physical safeguards.\textsuperscript{1612} Section 6802 establishes that financial institutions must not disclose to a non-affiliated third-party any non-public personal information unless that party provides a privacy notice.\textsuperscript{1613} The required notice must include, among other things, the names of people to whom the information may be disclosed, the nature of the information being collected, and the policies in place to protect the confidentiality and security of that information.\textsuperscript{1614}

When a financial institution seeks to disclose a consumer’s information, the consumer must be “given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party” and “given an explanation of how the consumer can exercise that nondisclosure option.”\textsuperscript{1615} The opportunity for the consumer to opt out is critical, and the GLBA mandates that all consumer information must remain redactable. Unless a credit reporting DApp uses an editable blockchain, such as the controversial Accenture project,\textsuperscript{1616} the immutability of the blockchain appears to directly contravene the redactability requirements of the GLBA.\textsuperscript{1617}

The GLBA limits the means of disclosure of non-public personal information, requires disclosure to consumers of privacy policies, and requires that consumers be given have an opt-out solution.\textsuperscript{1618} Blockchain technology would be a very efficient and accurate way to track information sharing with third parties, disclosures, and opt-outs. Compliance could also be ensured with standards through encrypted distributed ledger technology and private networks.

\textsuperscript{1611} 15 U.S.C. § 6801, et seq.
\textsuperscript{1612} 15 U.S.C. § 6801(b).
\textsuperscript{1613} 15 U.S.C. § 6802(a).
\textsuperscript{1615} 15 U.S.C. § 6802(b).
\textsuperscript{1616} Accenture, \url{www.accenture.com} (last visited Nov. 10, 2018); see generally Chapter 11 (Property).
\textsuperscript{1617} David Treat, \textit{Accenture: Absolute Immutability Will Slow Blockchain Progress}, CoinDesk (Nov. 10, 2016), \url{https://www.coindesk.com/absolute-immutability-will-slow-permissioned-blockchain-progress/}.
\textsuperscript{1618} 15 U.S.C. § 6802(a).
Once a solution is reached to enable customers to redact their information, blockchain technology promises to be a highly efficient way to track GLBA requirements.\textsuperscript{1619}

Chapter 13

13 Intellectual Property

13.1 Trademark and Copyright Laws

13.1.1 The Lanham Act

A trademark identifies a particular business as the source of a product and is a vital selling technique for consumers to identify with a trusted brand. A trademark can be a word, phrase, or symbol, such as a brand name, slogan, or logo. A service mark is a word, phrase, or symbol that is used to distinguish a service, while a trademark is used to distinguish a product. The term “trademark” is often used in a general sense to refer to both trademarks and service marks.

The Lanham Act, enacted in 1946, is the primary U.S. trademark statute. It prohibits, among other practices, trademark infringement, trademark dilution, and false advertising. The Trademark Law Revision Act (TLRA), enacted in 1988, provides that trademarks should be registered with the United States Patent and Trademark Office (USPTO) to establish rights of use and to protect against trademark infringement.

Registered trademarks are presumptively valid. Additionally, registration of a trademark with the USPTO serves as constructive notice of the registrant’s claim of ownership and allows the registrant to use the “®” symbol, obtain certain remedies not otherwise available from civil enforcement (e.g., treble damages and attorney fees from an infringer), and use the U.S. registration as the basis for applications abroad. Registration is at the discretion of the USPTO. The agency may refuse to register a trademark where the mark: lacks distinctiveness or is merely descriptive; is likely to be confused with a prior registered mark; is deceptive; is immoral or scandalous; disparages a person, institution, or belief; falsely suggests a connection with another institution, belief, or national symbol; consists of a flag of the United States; consists of a name identifying a living individual or the name, portrait, or signature of a deceased president of the United States during the life of his widow.

A trademark application must either include a verified statement that the mark is in use in U.S. commerce or that the applicant has a bona fide intent to use the mark in U.S. commerce. Unlike patents and copyrights, trademarks do not automatically expire after a certain number of years.

1623 15 U.S.C. § 1115(b); Sengoku Works Ltd. v. RMC Int’l, Ltd., 96 F.3d 1217, 1219-20 (9th Cir. 1996) (holding that an alleged infringer has the burden to overcome presumptive validity of a registered mark by a preponderance of the evidence).
years. Instead, trademark rights are based on actual “use” of the mark.\textsuperscript{1627} Once a trademark has been registered, to maintain trademark rights and prevent a finding that a trademark has been “abandoned,” the registrant must file with the USPTO both a statement of use and a specimen showing current use in U.S. commerce between the fifth and sixth anniversaries of the registration date.\textsuperscript{1628} The registration must then be renewed in the one-year period before the tenth anniversary of the registration and can be renewed every ten years thereafter, provided the registrant can then show current use in commerce.\textsuperscript{1629}

Unregistered trademarks are protectable under the Lanham Act as common law trademarks, but the protection is limited and only enforceable in the geographic region in which the trademark is known by customers.\textsuperscript{1630} Unlike registered trademarks, unregistered trademarks are not presumptively valid. Consequently, in an action for infringement of an unregistered trademark, the burden lies on the holder to prove that the trademark is valid.\textsuperscript{1631}

A trademark owner who believes its trademark is being infringed may file a civil suit for trademark infringement in state or federal court. To establish an infringement claim under the Lanham Act or common law, the plaintiff must demonstrate: (1) that it has a valid and legally protectable mark; (2) that it owns the mark; and (3) that the defendant’s use of the mark to identify goods or services causes a likelihood of confusion.\textsuperscript{1632}

The “party claiming ownership must have been the first to actually use the mark in the sale of goods or services.”\textsuperscript{1633} Thus, “a party pursuing a trademark claim must meet a threshold ‘use in commerce’ requirement.”\textsuperscript{1634} The Lanham Act defines “use in commerce” to mean “the \textit{bona fide} use of a mark in the ordinary course of trade, and not made merely to reserve a right in a mark.”\textsuperscript{1635}

\textsuperscript{1627} 15 U.S.C. § 1058.
\textsuperscript{1628} Id.
\textsuperscript{1629} Id.
\textsuperscript{1630} 15 U.S.C. § 1125; \textit{Emergency One, Inc. v. Am. Fire Eagle Engine Co.}, 332 F.3d 264, 267 (4th Cir. 2003) (“Common law determines who enjoys the exclusive right to use an unregistered trademark, the extent of such rights, and the proper geographical scope of any injunctive relief necessary to protect against the infringement of such rights.”); \textit{Time, Inc. v. Petersen Publ’g Co. L.L.C.}, 173 F.3d 113, 117 (2d Cir. 1999) (“The Act similarly prohibits the infringement of unregistered, common law trademarks.”).
\textsuperscript{1631} \textit{Tie Tech, Inc. v. Kinedyne Corp.}, 296 F.3d 778, 783 (9th Cir. 2002) (“[T]he registration is not absolute but is subject to rebuttal. In essence, the registration discharges the plaintiff’s original common law burden of proving validity in an infringement action.”); \textit{see also Manual of Model Civil Jury Instructions for the Ninth Circuit} 15.6 (2017) (setting forth elements and burden of proof in trademark cases) (quoting 15 U.S.C. § 1114(1)).
\textsuperscript{1632} \textit{A & H Sportswear, Inc. v. Victoria’s Secret Stores, Inc.}, 237 F.3d 198, 210 (3d Cir. 2000).
\textsuperscript{1633} \textit{Sengoku Works Ltd. V. RMC Int’l, Ltd.}, 96 F.3d 1217, 1219 (9th Cir. 1996).
\textsuperscript{1634} \textit{Rearden LLC v. Rearden Commerce, Inc.}, 683 F.3d 1190, 1203 (9th Cir. 2012).
\textsuperscript{1635} 15 U.S.C. § 1127.
The ‘likelihood of confusion’ analysis focuses on whether the use of the allegedly infringing mark leads to confusion as to the “source or sponsorship of the goods or services because of the marks used thereon.” According to a leading U.S. Supreme Court case, *San Francisco Arts & Athletics, Inc. v. United States Olympic Committee*, “confusion occurs when consumers make an incorrect mental association between the involved commercial products or their producers.” Although different jurisdictions have their own formulations of the test, courts generally consider a series of non-exclusive factors when determining a likelihood of confusion, including: (1) strength of the mark; (2) proximity of the goods, (3) similarity of the marks; (4) evidence of actual confusion; (5) marketing channels used; (6) type of goods and the degree of care likely to be exercised by the purchaser; (7) defendant’s intent in selecting the mark; and (8) likelihood of expansion of the product lines.

Regarding the strength factor, the “more unique the mark, the greater the degree of protection.” Thus, marks that are arbitrary or fanciful garner the highest degree of protection. A suggestive mark, one that requires a customer to “use imagination or any type of multistage reasoning to understand the mark’s significance,” receives less protection than arbitrary and fanciful marks. At the other end of the spectrum are descriptive marks and generic marks. A descriptive mark is one that “define[s] qualities or characteristics of a product in a straightforward way that requires no exercise of the imagination to be understood,” receives no trademark protection unless it acquires a secondary meaning – i.e., “if the public comes to associate the mark with a specific source.” Generic marks are not eligible for any trademark protection.

---

1639 *Survivor Media, Inc. v. Survivor Prods.*, 406 F.3d 625, 631 (9th Cir. 2005).
1640 “Arbitrary” marks are those that “use [] common words in a fictitious and arbitrary manner to create a distinctive mark which identifies the source of the product,” such as “Dutch Boy” paint. *Dreamwerks Prod. Grp., Inc. v. SKG Studio*, 142 F.3d 1127, 1131 n.7 (9th Cir. 1998).
1641 “A fanciful mark is a coined word or phrase, such as Kodak, invented solely to function as a trademark.” *Dreamwerks Prod. Grp., Inc. v. SKG Studio*, 142 F.3d 1127, 1131 (9th Cir. 1998).
1642 *Kendall-Jackson Winery, Ltd. v. E. & J. Gallo Winery*, 150 F.3d 1042, 1047 (9th Cir. 1998).
1643 *Id.* at 1047 n.8. Examples of suggestive marks include “Slickcraft” for boats, or “Air Care” for a service that maintains medical equipment for administering oxygen, or “Surfvivor” for beached-themed products. See *Airco, Inc. v. Air Prods. & Chemicals, Inc.,* 196 U.S.P.Q. 832 (TTAB1977); *AMF, Inc. v. Sleekcraft Boats*, 599 F.2d 341, 349 (9th Cir. 1979); *Survivor Media, Inc. v. Survivor Prods.*, 406 F.3d 625, 631-32 (9th Cir. 2005).
1644 Descriptive marks include “Honey Baked Ham” and “Honey Roast” nuts. *Kendall-Jackson Winery*, 150 F.3d at 1047 n.8.
1645 *Id.* at 1047 n.9.
The proximity-of-the-goods factor considers whether the goods or services of the competing marks are related. “Related goods (or services) are those ‘which would be reasonably thought by the buying public to come from the same source if sold under the same mark.” In Rearden LLC v. Rearden Commerce, Inc., the Ninth Circuit found that this factor weighed in favor of likelihood of confusion since the evidence suggested that the parties (1) offered similar technology platforms, (2) attended the same trade shows; (3) appeared in the same publications; and (4) relied on private investment funding from the same sources. In Survívivor Media, Inc. v. Survivor Products, the court concluded that, while both parties portrayed outdoor themes, customers were unlikely to associate the two products – Survívivor, which sold Hawaiian beach-themed products, and Survivor, which produced a reality TV show.

For the similarity factor, courts “analyze each mark within the context of other identifying features,” and “ask whether the marks are similar in sight, sound, and meaning.” In Survívivor Media, the Court found that the sound factor weighed in favor of the plaintiff (Survívivor) as the terms “Survívivor” and “Survivor” were almost phonetically identical. But the court also concluded that the sight and meaning factors did not suggest a likelihood of confusion because the defendant’s mark often is accompanied by the slogan “outwit[,] outplay[,] outlast,” and because Survívivor is a coined term referencing surfing, whereas Survivor means one who remains alive after others have not.

“Evidence of actual confusion by consumers is strong evidence of likelihood of confusion.” Such evidence can include customer surveys, letters from customers, testimony from manufacturing company owners that retailers were confused as to the source of products, testimony from a plaintiff’s employees that they were asked by consumers whether plaintiff and defendant were affiliated, misdirected emails intended for one party but sent to the other, and trade publications that questioned the possible relationship between plaintiff and defendant. Besides consumer confusion, courts consider confusion on the part of certain non-

1646 Rearden, 683 F.3d at 1212 (citations omitted).
1647 Both parties offered online services to clients to arrange business travel. Id.
1648 Id. at 1212-13.
1649 Survívivor Media, Inc. v. Survivor Prods., 406 F.3d 625 (9th Cir. 2005).
1650 Id. at 406 F.3d at 633.
1651 Id.
1652 Id.
1653 Id.
1654 Id.
1656 Id.
1657 Entrepreneur Media, Inc. v. Smith, 279 F.3d 1135, 1150 (9th Cir. 2002).
1658 Rearden, 683 F.3d at 1217.
1659 Id.
consumers, which can “(1) turn into actual consumer confusion (i.e., potential consumers); (2) serve as an adequate proxy or substitute for evidence of actual consumer confusion (i.e., non-consumers whose confusion could create an inference of consumer confusion); or (3) otherwise contribute to confusion on the part of the consumers themselves (i.e., non-consumers whose confusion could influence consumer perceptions and decision-making).”

Courts also look at “whether the parties distribute their goods in the same marketing channels.” In *Entrepreneur Media, Inc. v. Smith*, an infringement action brought by the publisher of “Entrepreneur” magazine against a public relations firm named EntrepreneurPR, the Ninth Circuit concluded that this factor did not weigh in the plaintiff’s favor because the parties’ marketing channels did not overlap to a significant degree: “[The parties] do not compete for subscribers, newsstand purchasers, or advertisers because *Entrepreneur Illustrated* is not for sale and does not feature paid advertisements.”

Additionally, courts consider the actions of consumers. “In analyzing the degree of care that a consumer might exercise in purchasing the parties’ goods, the question is whether a ‘reasonably prudent consumer’ would take the time to distinguish between the two product lines.” Courts “expect [a consumer] to be more discerning—and less easily confused—when he is purchasing expensive items.”

Courts also consider an alleged infringer’s intent. “[W]here the alleged infringer adopted his mark with knowledge, actual or constructive, that it was another's trademark,” courts will find a likelihood of confusion. An “intent to confuse consumers is not required for a finding of trademark infringement,” however, because the “[a]bsence of malice is no defense to trademark infringement.” Thus, the court found this factor in the plaintiff Survivor’s favor, because the defendant acknowledged awareness of the plaintiff’s mark prior to airing its Survivor show.

As for product expansion, courts look to whether one or both parties intend to expand their products or service lines into the types of products or services of the other. A “‘strong possibility’

---

1660 *Id.* at 1216; *Survivor Media*, 406 F.3d at 633 (“In analyzing this factor, we may consider whether merchants and non-purchasing members of the public, as well as actual consumers, were confused.”).

1661 *Survivor Media*, 406 F.3d at 633 (concluding that this factor weighed slightly in favor of Survivor because Hawaiian JC Penney Stores sold both parties’ merchandise).

1662 *Entrepreneur Media, Inc. v. Smith*, 279 F.3d 1135 (9th Cir. 2002).

1663 *Id.* at 1152.

1664 *Survivor Media*, 406 F.3d at 634 (noting that there is no clear standard for analyzing moderately priced goods, but that consumers are likely to exercise very little care for inexpensive goods).

1665 *Brookfield Commc'ns, Inc. v. W. Coast Entm't Corp.*, 174 F.3d 1036, 1060 (9th Cir. 1999).

1666 *Id.* at 1059.

1667 *Id.* (quoting *Dreamwerks Prod. Group v. SKG Studio*, 142 F.3d 1127, 1132 n.12 (9th Cir. 1998)).

1668 *Survivor Media*, 406 F.3d at 634.
that either party will expand his business to compete with the other or be marketed to the same consumers will weigh in favor of finding that the present use is infringing.”

13.1.2 The Trademark Counterfeiting Act of 1984

The Trademark Counterfeiting Act of 1984 (TCA) enhanced the protection provided by the Lanham Act by making the intentional or unauthorized use of a counterfeit trademark in connection with the trafficking of goods or services a criminal offense, and bolstered the Government’s enforcement remedies by allowing ex parte seizures.1670

To prove a violation of the TCA, “the government must establish that: (1) the defendant trafficked, or attempted to traffic, in goods or services; (2) such trafficking, or attempt to traffic, was intentional; (3) the defendant used a counterfeit mark on, or in connection with, such goods or services; and (4) the defendant knew the mark so used was counterfeit.”1671 For a first violation, an individual is subject to a maximum fine of $2,000,000 and/or 10 years’ imprisonment, while a non-individual is subject to a maximum fine of $5,000,000.1672 Penalties increase for subsequent violations – individuals are subject to a maximum fine of $5,000,000 and/or 20 years’ imprisonment, while non-individuals are subject to a $15,000,000 maximum fine.1673 The statute also prescribes fines and imprisonment if an individual knowingly or recklessly causes, or attempts to cause, serious bodily injury or death in connection with a violation.1674 Forfeiture, destruction, and restitution are also available remedies.1675

13.1.3 Copyright

The Copyright Act of 19761676 provides protection for authors of “original works of authorship,” including musical, artistic, literary, dramatic, and certain other types of intellectual work. The protection is available for both published and unpublished works. The Copyright Act gives authors exclusive rights in their original works, such as the right to (1) copy the copyrighted work; (2) prepare derivative works based on the copyrighted work; (3) distribute copies of the copyrighted work; (4) perform the copyrighted work; and (5) display the copyrighted work publicly.1677

1669 Homeowners Grp., Inc. v. Home Mktg. Specialists, Inc., 931 F.2d 1100, 1112 (6th Cir. 1991). Testimony that a party is interested in expanding its product line is insufficient. See Survivor Media, Inc. v. Survivor Prods., 406 F.3d 625, 634 (9th Cir. 2005) (“Although Deptula expressed interest in expanding his product line, mere speculation is not evidence”).


A copyright owner is entitled to bring a civil action for infringement against an alleged infringer.\textsuperscript{1678} To establish an infringement claim, the copyright owner must prove: “1) ownership of a valid copyright, and 2) copying of constituent elements of the work that are original.”\textsuperscript{1679}

A plaintiff may meet its burden under the first element by submitting a certificate of registration provided by the U.S. Copyright Office, which creates a rebuttable presumption that the copyright is valid.\textsuperscript{1680} The burden then shifts to the alleged infringer to challenge the validity by “offer[ing] some evidence or proof to dispute or deny the plaintiff's prima facie case of infringement.”\textsuperscript{1681} The alleged infringer may submit “evidence that the work had been copied from the public domain … or … that the work was a non-copyrightable utilitarian article.”\textsuperscript{1682} If the alleged infringer successfully rebuts the presumption of validity, the plaintiff must establish ownership of a valid copyright by showing: “(1) proof of originality and copyrightability and (2) compliance with the applicable statutory requirements.”\textsuperscript{1683}

Originality is proven “if the work is independently created by the author and possesses some minimal degree of creativity.”\textsuperscript{1684} “[T]he requisite level of creativity is extremely low; even a slight amount will suffice. … [A] work may be original even though it closely resembles other works so long as the similarity is fortuitous, not the result of copying.”\textsuperscript{1685}

Copyrightability exists for “original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.”\textsuperscript{1686} However, no protection is given to an “idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or

\textsuperscript{1678} 17 U.S.C. § 501(b).
\textsuperscript{1680} 17 U.S.C. § 410(c).
\textsuperscript{1681} \textit{Entm’t Res. Group, Inc. v. Genesis Creative Group, Inc.}, 122 F.3d 1211, 1217 (9th Cir. 1997).
\textsuperscript{1682} \textit{Fonar Corp. v. Domenick}, 105 F.3d 99, 104 (2d Cir. 1997) (citing \textit{Folio Impressions, Inc. v. Byer Cal.}, 937 F.2d 759, 764 (2d Cir. 1991); \textit{Carol Barnhart Inc. v. Econ. Cover Corp.}, 773 F.2d 411, 414 (2d Cir. 1985).
\textsuperscript{1683} \textit{Compaq Computer Corp. v. Ergonome Inc.}, 387 F.3d 403, 408 (5th Cir. 2004); \textit{Darden v. Peters}, 488 F.3d 277, 285 (4th Cir. 2007); \textit{Syntek Semiconductor Co. v. Microchip Tech. Inc.}, 307 F.3d 775, 781 (9th Cir. 2002).
\textsuperscript{1684} \textit{Reece v. Island Treasures Art Gallery, Inc.}, 468 F. Supp. 2d 1197, 1202 (D. Haw. 2006) (“Almost any photograph may claim the necessary originality to support a copyright merely by virtue of the photographer's personal choice of subject matter, angle of photograph, lighting, and determination of the precise time when the photograph is to be taken.”) (quotation omitted).
\textsuperscript{1685} \textit{Feist Publ’n’s}, 499 U.S. at 345-46.
\textsuperscript{1686} 17 U.S.C. § 102(a).
The Copyright Act provides a non-exhaustive list of works that may be copyrighted:

1) Literary works;
2) Musical works, including any accompanying words;
3) Dramatic works, including any accompanying music;
4) Pantomimes and choreographic works;
5) Pictorial, graphic, and sculptural works;
6) Motion pictures and other audiovisual works;
7) Sound recordings; and
8) Architectural works.  

9) Computer programs are protected as literary works.

A copyright owner may not institute a civil action for infringement “until preregistration or registration of the copyright claim has been made in accordance with this title.”  “[A] plaintiff has complied with all statutory formalities for copyright registration when the U.S. Copyright Office receives the plaintiff’s application for registration, fee, and deposit.”

To establish the second element of copyright infringement, “copying of constituent elements of the work,” a plaintiff must provide proof of: (1) actual copying of the work by the defendant, and (2) “that the copying was so extensive that it rendered the infringing and copyrighted works substantially similar.”

Federal courts have articulated varying standards for substantial similarity. The First, Second, Third, Fifth, and Seventh Circuits apply an “ordinary observer” test: “Works can be substantially similar despite the presence of disparities. The key is whether ‘the ordinary observer, unless he set out to detect the disparities, would be disposed to overlook them, and regard [the

---

1689 The Copyright Act defines “computer program” as “a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.” 17 U.S.C. § 101.
1690 *Spear Mktg., Inc. v. BancorpSouth Bank*, 791 F.3d 586, 597 (5th Cir. 2015) (holding “computer software is a tangible medium protected by the Copyright Act”); *Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339, 1354 (Fed. Cir. 2014) (“It is undisputed that computer programs … can be subject to copyright protection as ‘literary works.’”).
1692 *Geoscan, Inc. of Texas v. Geotrace Techs., Inc.*, 226 F.3d 387, 393 (5th Cir. 2000).
1693 *Johnson v. Gordon*, 409 F.3d 12, 18 (1st Cir. 2005).
works’] aesthetic appeal as the same."\textsuperscript{1694} For the ordinary observer test, expert testimony is not permitted.\textsuperscript{1695}

Other courts, including the Fourth, Eighth, and Ninth Circuits, use the “total concept and feel test,” also known as the “extrinsic/intrinsic test.”\textsuperscript{1696} The extrinsic part of the test “requires plaintiffs to show overlap of concrete elements based on objective criteria,”\textsuperscript{1697} such as “the type of artwork involved, the materials used, the subject matter, and the setting for the subject.”\textsuperscript{1698} The “intrinsic test is subjective and asks whether the ordinary, reasonable person would find the total concept and feel of the works to be substantially similar.”\textsuperscript{1699} Expert opinion is only allowed to assist the trier of fact for the extrinsic component of the test, not the intrinsic.\textsuperscript{1700}

A third group of courts, including the Sixth and Tenth Circuits, use the “abstraction-filtration-comparison” test, which has been described as follows:

we separate the ideas (and basic utilitarian functions), which are not protectable, from the particular expression of the work. Then, we filter out the nonprotectable components of the product from the original expression. Finally, we compare the remaining protected elements to the allegedly copied work to determine if the two works are substantially similar.\textsuperscript{1701}

For computer programs, which are often complex and unfamiliar to most members of the public, some courts have analyzed whether the programs at issue are substantially similar based on a totality of evidence, including both lay and expert testimony, to “make a qualitative, not quantitative, judgment about the character of the work as a whole and the importance of the substantially similar portions of the work.”\textsuperscript{1702}


\textsuperscript{1695} Segrets, Inc. v. Gillman Knitwear Co., 207 F.3d 56, 66 (1st Cir. 2000); Arnstein v. Porter, 154 F.2d 464, 468 (2d Cir. 1946).

\textsuperscript{1696} Lyons P'ship, L.P. v. Morris Costumes, Inc., 243 F.3d 789, 801 (4th Cir. 2001); Moore v. Columbia Pictures Indus., Inc., 972 F.2d 939, 945 (8th Cir. 1992); Unicorns, Inc. v. Urban Outfitters, Inc., 853 F.3d 980, 985 (9th Cir. 2017).

\textsuperscript{1697} Unicorns, Inc. v. Urban Outfitters, Inc., 853 F.3d 980, 985 (9th Cir. 2017).

\textsuperscript{1698} Sid & Marty Krofft Television Prods., Inc. v. McDonald's Corp., 562 F.2d 1157, 1164 (9th Cir. 1977).

\textsuperscript{1699} Unicorns, Inc. v. Urban Outfitters, Inc., 853 F.3d 980, 985 (9th Cir. 2017).

\textsuperscript{1700} Sid & Marty Krofft Television Prods., 562 F.2d at 1164.

\textsuperscript{1701} Bridgeport Music, Inc. v. UMG Recordings, Inc., 585 F.3d 267, 274-75 (6th Cir. 2009); Country Kids 'N City Slicks, Inc. v. Sheen, 77 F.3d 1280, 1285 (10th Cir. 1996).

\textsuperscript{1702} Whelan Assocs., Inc. v. Jaslow Dental Lab., Inc., 797 F.2d 1222, 1232-33, 1245 (3d Cir. 1986). See also Computer Assocs. Intl', Inc. v. Altai, Inc., 982 F.2d 693, 713 (2d Cir. 1992)
An alleged infringer may raise the defense of “fair use” against a claim for copyright infringement. The statute expressly contemplates the fair use of copyrighted work for news reporting, criticism, teaching, scholarship, or research purposes, but these are merely illustrative.1703 The Copyright Act sets forth four factors relevant to the fair use analysis: (1) the purpose and character of the use; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion of the original work; and (4) the effect of the use upon the market.1704

When considering the purpose and character of the use, courts focus on whether the material has been used to create something completely new or transformative, and whether such creation was intended for commercial gain or nonprofit educational purposes.1705 Courts have found a transformative purpose both where the defendant combines copyrighted expression with original expression to produce a new creative work, and where the defendant uses a copyrighted work in a different context to serve a different function than the original.1706 As one court explained:

[C]ourts will not sustain a claimed defense of fair use when the secondary use can fairly be characterized as a form of commercial exploitation, i.e., when the copier directly and exclusively acquires conspicuous financial rewards from its use of the copyrighted material. Conversely, courts are more willing to find a secondary use fair when it produces a value that benefits the broader public interest. The greater the private economic rewards reaped by the secondary user (to the exclusion of broader public benefits), the more likely the first factor will favor the copyright holder and the less likely the use will be considered fair.1707

Courts are typically lenient toward nonprofit and educational reproductions of material because the purpose is not to gain profit off the reproduction of the work of another.1708 However,
not all nonprofit uses are considered fair use. As the Eleventh Circuit cautioned, “care must be taken not to allow too much educational use, lest we undermine the goals of copyright by enervating the incentive for authors to create the works upon which students and teachers depend.”

In *Warner Bros. Entertainment, Inc. v. RDR Books*, the defendant claimed its “Lexicon” book was a fair use of the *Harry Potter* works. The court determined that the Lexicon, as compared to the *Harry Potter* series, was transformative as it served a reference purpose whereas the *Harry Potter* series primarily served entertainment and aesthetic purposes. The court also found, however, when comparing the plaintiff’s companion books to the *Harry Potter* series, the defendant’s work was only “slightly transformative.” The court acknowledged that the companion books had both an entertainment and informational purpose, but ultimately concluded that the defendant’s work was still somewhat transformative because “it adds a productive purpose to the original material by synthesizing it within a complete reference guide that refers readers to where information can be found in a diversity of sources.”

The “nature of the work” factor is concerned with the idea that the dissemination of facts is informative and beneficial for the public, and thus gives more leeway for others to copy from factual works, such as biographies, than from fictional works. There is a stronger fair use argument if the copied material comes from a published than from an unpublished work because authors have the right to control the first public appearances of their expression.

The “amount and substantiality” factor considers “whether ‘the amount and substantiality of the portion used in relation to the copyrighted work as a whole,’ … are reasonable in relation to the purpose of the copying.” The less that is taken from the original work, the more likely fair use will serve as a defense. Where the work has been copied verbatim, courts generally do not find circumstances where it would be unreasonable to require permission.”

---

1709 *Cambridge Univ. Press v. Patton*, 769 F.3d 1232, 1264 (11th Cir. 2014) (discussing cases in which “court[s] refused to allow the defendants, who were engaged in commercial operations, to stand in the shoes of students and professors in claiming that their making of multiple copies of scholarly works was for nonprofit educational purposes.”).


1711 *Id.* at 542.

1712 *Id.*

1713 *Cambridge Univ. Press v. Patton*, 769 F.3d 1232, 1268 (11th Cir. 2014) (“In contrast, ‘[t]he law generally recognizes a greater need to disseminate factual works than works of fiction or fantasy,’ and so it is more likely that the use of a factual or informational work will be fair use.”) (quoting *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 563 (1985)).

1714 *Harper & Row*, 471 U.S. at 555 (“Under ordinary circumstances, the author's right to control the first public appearance of his undisseminated expression will outweigh a claim of fair use.”).

1715 *Campbell*, 510 U.S. at 586.
fair use.\textsuperscript{1716} However, this rule is not necessarily true in cases of parody. As the Supreme Court acknowledged in \textit{Campbell v. Acuff-Rose Music}, a parody relies on its “recognizable allusion to its object through distorted imitation,” meaning “the parody must be able to ‘conjure up’ at least enough of that original work to make the object of its critical wit recognizable.”\textsuperscript{1717} Thus, use of recognizable parts of the original work, even verbatim, may be permitted for parodies. However, the Supreme Court cautioned:

> Once enough has been taken to assure identification, how much more is reasonable will depend, say, on the extent to which the song's overriding purpose and character is to parody the original or, in contrast, the likelihood that the parody may serve as a market substitute for the original.\textsuperscript{1718}

The factor relating to the effect of use upon the potential market is primarily concerned with whether the infringing use deprives the original copyright owner of income, or undermines a new or potential market for copyrighted work.

Penalties for violation of copyright law are severe.\textsuperscript{1719} A copyright owner who succeeds in a civil infringement action is entitled to either its actual damages plus the infringer’s profits from the infringement, or statutory damages up to a maximum of $30,000 per work or $150,000 if the infringement was willful.\textsuperscript{1720} A court can also enjoin the infringing acts,\textsuperscript{1721} impound\textsuperscript{1722} the illegal works, and award costs and reasonable attorneys’ fees to the prevailing party.\textsuperscript{1723}

\begin{itemize}
\item \textsuperscript{1716} \textit{Harper & Row}, 471 U.S. at 565 (“Conversely, the fact that a substantial portion of the infringing work was copied verbatim is evidence of the qualitative value of the copied material, both to the originator and to the plagiarist who seeks to profit from marketing someone else's copyrighted expression.”); \textit{Rosemont Enters., Inc. v. Random House, Inc.}, 366 F.2d 303, 310 (2d Cir. 1966) (“The fair use privilege is based on the concept of reasonableness and extensive verbatim copying or paraphrasing of material set down by another cannot satisfy that standard.”); \textit{RDR Books}, 575 F. Supp. 2d at 513 (finding that the “slightly transformative” quality of the defendant’s work was insufficient to justify fair use in light of the extensive verbatim use of ideas and phrases from plaintiff’s Harry Potter books.).
\item \textsuperscript{1717} \textit{Campbell}, 510 U.S. at 588.
\item \textsuperscript{1718} \textit{Id.; see also Henley v. DeVore}, 733 F. Supp. 2d 1144, 1161 (C.D. Cal. 2010) (concluding that the defendant’s song, which “took virtually everything,” “was excessive in relation to the parodic element” of lampooning singer Don Henley).
\item \textsuperscript{1719} 17 U.S.C. §§ 501-05.
\item \textsuperscript{1720} 17 U.S.C. §§ 504.
\item \textsuperscript{1721} 17 U.S.C. §§ 502.
\item \textsuperscript{1722} 17 U.S.C. §§ 503.
\item \textsuperscript{1723} 17 U.S.C. §§ 505.
\end{itemize}
In addition to civil liability, a person who willfully infringes a copyright can be prosecuted criminally and is subject to imprisonment for one to 10 years depending on the specific criminal conduct and number of violations, and/or a fine of up to $250,000.

13.1.4 Copyright Protection for Derivative Works

The Copyright Act permits the owner of a copyrighted work to prepare or authorize derivative works based on that work. A derivative work is “a work based upon one or more preexisting works.” Derivative works may be entitled to copyright protection so long as the author’s contributions do not infringe on the rights of the owner of the original work. The copyright in a derivative work extends only to the material contributed by the author of the derivative work, which is distinguished from the preexisting material and implies no exclusive right in the preexisting material. Modification of the original must be substantial for the derivative work to be considered original in its own right and merit copyright protection.

With respect to computer programs, the Copyright Act limits some rights of copyright owners. Specifically, owners of copies of programs are allowed to make new copies or adaptations of those programs, provided:

1724 17 U.S.C. § 506 (“Any person who willfully infringes copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed … by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution.”).

1725 18 U.S.C. § 2319. Length of imprisonment varies depending on whether the offense is the first offense or subsequent offense, and if the infringement was committed for any of the reasons set forth in 17 U.S.C. § 506.


1729 Dynamic Sols., Inc. v. Planning & Control, Inc., 646 F. Supp. 1329, 1340 (S.D.N.Y. 1986) (“Copyright protection does not extend to any part of the derivative work in which pre-existing material was used unlawfully—for example, if the copyrighted portions of the pre-existing work were used without the owner's permission.”); Schrock v. Learning Curve Int'l, Inc., 586 F.3d 513, 518 (7th Cir. 2009) (“The Copyright Act specifically grants the author of a derivative work copyright protection in the incremental original expression he contributes as long as the derivative work does not infringe the underlying work.”).

1730 17 U.S.C. § 103(b).

1731 Knickerbocker Toy Co. v. Winterbrook Corp., 554 F. Supp. 1309, 1317-18 (D.N.H. 1982) (“The original aspects of the derivative work must themselves be nontrivial, and the copyright in the derivative work does not affect the copyright protection in the underlying work.”).
1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine, and that it is used in no other manner; or

2) that such a new copy or adaptation is for archival purposes only, and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful.\textsuperscript{1732}

Courts determine ownership of a copy of a computer program by looking at the incidents of ownership, of which title to the program is but one factor.\textsuperscript{1733} In determining whether a copy or adaptation is “an essential step in the utilization of the computer program in conjunction with a machine,” courts consider whether it is “essential to allow use of the program[s] for the very purpose for which [they were] purchased.”\textsuperscript{1734} Courts analyze whether a copy or adaptation is “used in no other manner” by focusing on the “use envisioned in the creation of the program.”\textsuperscript{1735}

13.2 Blockchain as an IP Registry

Currently, copyrights, trademarks, and patents are primarily recorded and viewed on various registries around the world with no centralized catalogue of works – or often with no registration at all. Consequently, ownership is hard to prove, authors have difficulty knowing who is using their work, and third parties who wish to use a piece of a work face challenges determining

\textsuperscript{1732} 17 U.S.C. § 117(a).

\textsuperscript{1733} \textit{Krause v. Titleserv, Inc.}, 402 F.3d 119, 123-24 (2d Cir. 2005) (determining the defendant was the owner of computer programs developed by the plaintiff because (1) the defendant paid substantial consideration for the development of the programs for its benefit; (2) the plaintiff customized the program to the defendant’s operations; (3) copies of the program were saved in the defendant’s servers; and (4) the parties’ agreement provided that the defendant was allowed to possess and use the program forever); \textit{see also DSC Commc’ns Corp. v. Pulse Commc’ns, Inc.}, 170 F.3d 1354, 1361 (Fed. Cir. 1999) (concluding that Regional Bell Operating Companies were not the owners of copies of computer program pursuant to 17 U.S.C. § 117 because the agreements between the RBOCs and the party claiming infringement characterized the RBOCs as non-owners and included terms that were “inconsistent with the rights normally enjoyed by owners of copies of software.”).

\textsuperscript{1734} \textit{Krause}, 402 F.3d at 125 (citation and internal quotation marks omitted). In \textit{Krause}, the Second Circuit determined that this test was met where the modifications were for (1) fixing “bugs,” (2) changing source code to add new clients and client information, (3) incorporating the programs into defendant’s Windows-based system, and (4) adding capabilities like the ability to print checks and to allow customers to access their records. \textit{Id.} at 125-26; \textit{see also Softech Worldwide, LLC v. Internet Tech. Broad. Corp.}, 761 F. Supp. 2d 367, 374 (E.D. Va. 2011) (concluding the defendant’s modifications to computer programs, which maintained the programs’ usefulness, were essential steps in the utilization of the programs).

\textsuperscript{1735} \textit{Krause}, 402 F.3d at 129-30 (concluding the defendant’s modifications that allowed its customers to access the disputed computer programs fell within the intended use of the programs, which “were designed for the processing of transactions relating to [the defendant’s] relationship with its customers.”).
where and from whom to obtain a license. Authors are often unable to prevent infringements of their work or to maximize profits from it.\footnote{1736 Suzy Shinner, \textit{Blockchain Technology and IP}, TaylorWessing (Mar. 2017), \url{https://www.taylorwessing.com/download/article-blockchain-technology-and-ip.html}.}

Considering the low cost of maintenance, transparency, lessened administrative burden, and resistance to fraud due to its immutability, distributed ledger technology is ideal for creating public shared databases that record and track transactions and assets. Through decentralized applications (DApps) on networks such as Ethereum, blockchain technology has the ability to expand from a virtual currency transaction ledger to a registry tool that can track the rights and transactions attached to all manner of digital creative works, from books to music to artwork.\footnote{1737 NexChange, \textit{Can Blockchain Tech Revolutionise IP and Digital Content?} (2015), \url{https://nexchange.com/article/4012}.}

DApp copyright platforms such as Bernstein and Binded (Binded is formerly known as Blockai) have been created for this exact purpose – i.e., allowing authors to record copyright ownership, which can then be monitored to see where and how the work is used on the Internet, and making it far easier for third parties to seek licenses.\footnote{1738 Binded: About, \url{https://binded.com/about} (last visited Oct. 10, 2018); Bernstein, \url{https://www.taylorwessing.com/download/article-blockchain-technology-and-ip.html} (last visited Oct. 10, 2018).} Both applications give the author of the copyright a digital certificate of authenticity when created, including details of ownership and a timestamp (a method for publishing the creation of an idea or concept without necessarily revealing details) to prove that the work was published at a specific time and that action was taken to make it secure.\footnote{1739 Nathan Lands, \textit{What You Get when You Register a Copyright}, Binded \url{https://help.binded.com/features/vault/copyright-certificate} (last updated Oct. 2018).} Currently, if an author uploads his or her work to the Internet, it is difficult to maintain control of it and monitor who is using it and for what purpose. Blockchain technology can be used to provide a single, public, global database with complete immutability. Even large companies such as Kodak are recognizing how blockchain technology can assist photographers in maintaining control over their intellectual property. In 2017, Kodak licensed its brand name to WENN Digital for the creation of a platform where KODAKCoin is used as a method of paying for permission to use photographs on the platform.\footnote{1740 Brad Jones, \textit{Kodak Cryptocurrency and Blockchain Ledger Will Help Photographers Protect Their Copyright}, Futurism (Jan. 10, 2018), \url{https://futurism.com/kodak-cryptocurrency-blockchain-ledger-help-photographers-protect-copyright/}.}

The immutability of blockchain technology makes it a perfect solution for an IP registry; once the record of ownership is added to the distributed ledger, it is there forever and will never change. There can be no allegations of incorrect or altered entries in lawsuits surrounding ownership. Blockchain also offers possibilities for licensing works by creating a direct link between the authors and the users, thereby reducing the costs of transactions and liaising through
third parties. A global searchable database showing transactions would greatly reduce the costs of searching for ownership.\textsuperscript{1741}

Executable distributed code contracts (EDCCs) are decentralized computer protocols used to execute contractual agreements, and could be beneficial in the licensing and sale of IP rights.\textsuperscript{1742} Following the execution of an EDCC, the programming could be coded to instruct the automatic registration of licenses and to send emails and notifications to all relevant parties. In addition, where the use of a piece of work is registered on the blockchain, the author could have pre-programmed EDCCs that automatically charge the user a pre-determined amount for each piece of work used. EDCCs can also be tied into micropayments for use of the work by assigning a virtual currency wallet address and then allowing the user to make a payment to the author in return for the use. This method would be far simpler and more transparent than current royalty and licensing payment systems, which are administered by different organizations in different countries for different types of works,\textsuperscript{1743} and the method would lead to lower costs and easier access to the use of the works.\textsuperscript{1744}

Cognate, a blockchain-based trademark documentation and protection platform,\textsuperscript{1745} allows for the relatively inexpensive registration of common law trademarks in less than 10 minutes, as opposed the USPTO registration process, which often takes up to 10 months and is much more costly.\textsuperscript{1746} While blockchain trademark registries like Cognate currently only register common law trademarks, the ability to timestamp and receive certification of ownership provides solid evidence rebutting the presumption of invalidity. Cognate also offers the ability to monitor a registered trademark and uses innovative machine learning algorithms to instantly analyze possible infringements, sending automatic email alerts where the marks are found to be alike.\textsuperscript{1747}

\textsuperscript{1741} Bryant Nielson, \textit{Blockchain & Ownership of Intellectual Property}, Your Training Edge (Nov. 14, 2016), \url{http://www.yourtrainingedge.com/blockchain-ownership-of-intellectual-property/}.


\textsuperscript{1743} For example, just in the United States, users who want to use pre-existing music may have to pay royalties and fees to the American Society of Composers, Authors and Publishers; Broadcast Music, Inc.; Asociacion de Compositores y Escritores de la Musica Latinoamericana; and the Society of European Stage Authors and Composers. Additionally, they must pay royalties to SACEM in France, SABAM in Belgium, GEMA in German, and JASRAC in Japan. With respect to digital music, SoundExchange is a non-profit organization that collects and distributes royalties for licenses for lyrics and scores, as well as for streaming the sound recording.

\textsuperscript{1744} See Shinner, \textit{supra} note 1736.


possibilities of global reach for such a database may ultimately take the place of far less efficient government registries, like the USPTO registry.

Blockchain technology can also help companies establish whether their trade secrets have been misappropriated, because it allows for timestamping. As with other forms of intellectual property, in subsequent litigation, when establishing initial ownership, this information will play a vital role in protecting the organization’s interests in its proprietary technology and business methods. Again, unlike conventional methods of digital timestamping, which use a centralized server, the timestamp on a blockchain is guaranteed to never change.

### 13.3 Software Developer Rights and Licensing

‘Source code’ refers to the statements or instructions written by a programmer in a programming language using a text editor or visual programming tool. Once written, the files containing the source code are assembled and translated from the programming language into binary code by a special software program called a ‘compiler.’ The output from the compiler is called the ‘object code,’ which cannot be easily read or understood by humans as it consists mainly of binary numbers (0s and 1s). Generally, the copy of software programs that consumers buy contain object code, not source code, as software companies do not want users to have the ability to manipulate their programs.

Software, including both object and source codes, is protected as a literary work under U.S. copyright law. Thus, programmers unfamiliar with copyright or contract law who incorporate portions of copyrighted code into their own code, as is common, could face surprising civil and criminal penalties.

#### 13.3.1 Free and Open Source Software

The source code used by large technology companies, such as Facebook, Twitter, and Microsoft, is proprietary and protected by copyright law; and a programmer who uses this source code without permission can be subject to civil damages and criminal penalties. In contrast, free and open source software (FOSS) is developed by informal networks of programmers with the intent to advance technological innovation through collaboration.

The free software movement was begun in 1983 by computer scientist Richard Stallman, who launched the GNU project. GNU was developed as a replacement for the UNIX operating system, which historically has operated through proprietary licenses. The GNU project respects

---


1750 Id.

1751 See Id.

1752 Stern Elecs., Inc. v. Kaufman, 669 F.2d 852, 855 (2d Cir. 1982); Williams Elecs., Inc. v. Artic Intl’, Inc., 685 F.2d 870, 876 (3d Cir. 1982).

the freedom of computer users by allowing them to access and modify source code. 1754 The source code is licensed free of charge, enabling anyone to use, copy, study, and change the software. 1755

FLOSS significantly decreases software costs by circumventing the necessity to buy expensive code, and often increases security and stability through the implementation of universal code, affording developers greater privacy and control over their hardware. The free software ethos is sometimes referred to as “free (libre) open source software,” or FLOSS, to emphasize that “free” software refers to freedom and not price. 1756 The free software movement does not, however, prevent developers from developing their own products from the “free” source code and charging for those products.

The two largest blockchain networks, Bitcoin and Ethereum, both utilize free and open source software. Ethereum’s terms and conditions expressly include a notice of risk that an alternative Ethereum-based network could be established using the same open source code and negatively impact the Ethereum platform through competition. 1757 The legal agreement provides notice of risk of security weaknesses or bugs, which may be introduced by the Ethereum team or other third parties who modify the core infrastructural elements of the Ethereum platform source code, and which may cause the system to lose Ether stored in user accounts. 1758

Networks within the blockchain community have mostly encouraged open source in a bid to increase network transparency. The Linux Foundation started the Hyperledger Project in 2015 to support open source blockchains through the advancement of cross-industry collaboration, with a focus on improving aspects of performance and reliability of the blockchain networks. The project aims to act as an “umbrella” for software communities by bringing together a number of independent efforts to develop open protocols and standards through a modular framework that supports different components and uses. 1759 One of the driving needs for such collaboration is the global talent shortage for developers who understand cryptocurrency engineering challenges, some of whom are working independently on the same projects, thereby needlessly duplicating work. The Hyperledger Project aims to build opportunities for developers to work on common open source software.

---

1756 Stallman, supra note 1756.
1758 Id.
source code and roadmaps whenever possible. In April 2017, Hyperledger’s Technical Steering Committee accepted Monax “Burrow” codebase into the project, which was the first Ethereum-compatible blockchain to be accepted by the Hyperledger. The Burrow code is published on Hyperledger’s GitHub.

13.3.2 Licensing

For a piece of software to be considered open, access to the source code alone is insufficient; specific distribution terms must comply with set criteria. The open source license should not restrict any party from selling or gifting the software as a component of an aggregate software distribution, and must not require a royalty or other fee for such a sale. The software must include source code and allow distribution in source code as well as compiled form, or there must be a well-publicized means of obtaining the source code. Moreover, the source code must be in a form that allows a programmer to modify the program; deliberately obfuscated source code is not allowed.

The open source license must allow derived works and modifications with the same distribution terms as the original software. An exception exists where the original license allows the distribution of “patch files” containing the source code for the purpose of modifying the program at a time.

The open source license cannot discriminate against any person, group of persons, or specific field of endeavor. The rights attached to the program must apply following redistribution, without need for additional license, and the rights must not depend on the program’s being part of a particular software distribution. The license must not restrict other software that is distributed with the licensed software, and no provision may be predicated on any individual technology or style of interface.

---


1763 Id.

1764 Id.

1765 Id.

1766 Id.

1767 For example, the license must not restrict the program from use in a business, or from use in genetic research.

1768 Id.

1769 Id.
13.3.3 Copyleft

Copyleft is the practice of offering the right to distribute modified versions of work product with the mandate that the same rights be preserved in any further derivative works.\textsuperscript{1770} Copyleft licenses are protective or reciprocal. They are not the same as permissive free software licenses. The easiest way to make software free is simply to put it in the public domain uncopyrighted, but this allows people to edit the software and convert it into proprietary software. When a piece of software is “copylefted,” it is not put into the public domain but distributed with stipulations that any redistribution must remain free and must allow for the freedom to further copy and change it. To copyleft a program, the licensor first states that it is copyrighted then adds distribution terms giving anyone the right to use, modify, and redistribute the code or any program derived from it, but only if the distribution terms are unchanged.\textsuperscript{1771} Thus, the freedom and the code become legally inseparable.

The name ‘copyleft’ is meant to signify that such licenses guarantee all users’ freedom to use the subject source code, in contrast to the copyright, which restrict users’ ability to use source code. The most common copyleft license is the GNU General Public License (GPL).\textsuperscript{1772} Originally released in 1989 by the Free Software Foundation for the GNU project, the GPL is widely utilized today and grants recipients of a computer program the rights enumerated in the definition of free software. Specifically, GPL provides four essential freedoms inherent in free software: (1) the freedom to run the program as you wish; (2) to study how the program works and adapt it; (3) to redistribute copies so you can help your neighbor; and (4) to improve the program and release your improvements to the public so the whole community benefits.\textsuperscript{1773}

Re-usable code is a key component of any developer’s toolkit, and is essential for both technological growth and creation of a profitable software development business. Prominent software programs licensed under the GPL include the GNU Compiler Collection and the Linux Kernel. The success of Linux-based systems is largely attributed to the copyleft provided by GPL, which afforded contributing programmers the assurance that their work would remain free and benefit the whole world rather than be exploited by software companies that generally operate to make profits for their investors and shareholders.\textsuperscript{1774}

The GPL license is quite strict. If a developer uses a single line of code from GPL-licensed software in his or her software, then that software cannot be closed source and must remain free.\textsuperscript{1775} This requirement is enforced by copyright attorneys serving as general counsel for the Free

---


\textsuperscript{1771} Id.

\textsuperscript{1772} GNU,\textit{ GNU General Public License}, GNU Operating System (Jun. 29, 2007), \url{https://www.gnu.org/licenses/gpl-3.0.en.html}.


\textsuperscript{1774} GNU,\textit{ supra} note 1770.

\textsuperscript{1775} Id.
Software Foundation; they receive reports of GPL-license violations, conduct further investigation into the source code to verify the violation, then contact the violating party to provide advice on how to correct the error.\footnote{1776}

GNU Affero GPL (AGPL) was designed as an alternate form of copyleft for software programs that are likely to be used on servers.\footnote{1777} The license was originally designed by Affero in 2002 with the purpose of closing a perceived application service provider (ASP) loophole discovered in the ordinary GPL.\footnote{1778} Later versions of the GPL closed this loophole. AGPL ensures modified versions of software that are used to implement services available to the public are released as source code to the public.\footnote{1779} GNU Lesser GPL (LGPL), a compromise between GNU and the more permissive licenses discussed below, allows developers to use and integrate software released under the LGPL license into their own (often proprietary) software without the requirement to release the source code. As the word “lesser” suggests, LGPL does not guarantee complete freedom in use of software, merely the freedom of modification for those components licensed under the LGPL.\footnote{1780}

### 13.3.4 BSD and MIT Licenses

The reciprocity share-alike requirements of the GPL differ from those of permissive free software licenses, such as the Berkeley Standard Distribution (BSD) and MIT licenses. The BSD license was created in 1975 as a simple and liberal license for UNIX computer software. The only restrictions placed on users of software under a typical BSD license apply if the software is redistributed in any form, with or without modification.\footnote{1781} In that instance, the BSD requires users to include in the redistribution the original copyright notice, a list of two simple restrictions, and a disclaimer of liability.\footnote{1782} This ensures that users of the software cannot claim that they authored the original source code and that they cannot sue the original developer if the software that they chose to copy does not function as expected.


\footnote{1777}{*GNU Affero General Public License*, GNU Operating System (Nov. 19, 2007), \url{https://www.gnu.org/licenses/agpl-3.0.en.html}.}

\footnote{1778}{There was a fear that copyleft provisions would not apply if programmers who used the source code did not distribute the resulting software. GNU, *Why the Affero GPL*, GNU Operating System, \url{https://www.gnu.org/licenses/why-affero-gpl.html} (last updated May 10, 2015).}

\footnote{1779}{See *Affero General Public License*, supra note 1777.}


\footnote{1782}{Open Source Initiative, *The 3-Clause BSD License*, \url{https://opensource.org/licenses/BSD-3-Clause} (last visited Sept. 26, 2018).}
Some BSD licenses also include a clause restricting the use of the name of the software for endorsing or promoting derivative works. In contrast to the GPL, BSD licenses do not require that derivative works remain freely available, allowing for the direct incorporation of code from open source projects into closed source or proprietary projects.\(^{1783}\) Thus, source code licensed under a BSD license can be freely modified and used in proprietary derivative works. The license is particularly useful where a programmer wants to create a commercial product from open source code but wants to ensure that his or her modifications remain secret.\(^{1784}\)

The MIT license contains only a single limited restriction on reuse and distribution – that all future copies of the licensed software include a copy of the MIT license terms and copyright notice.\(^{1785}\) Unlike the BSD license, the MIT license is widely compatible with the GPL.\(^{1786}\) A programmer can take a piece of MIT-licensed software and then license it freely under the GPL. For example, jQuery, the JavaScript library, was dual-licensed under both GPL and MIT for many years to allow users maximum flexibility and to give them the ability to use whichever license suited their projects best. jQuery subsequently opted to remove the GPL because using a single license made it far easier for the jQuery Foundation to manage and eliminated the confusion that existed concerning its dual-licensing policy, such as whether software users had to comply with both licenses. jQuery, however, has maintained that users are still free to take a jQuery Foundation project, make changes, and relicense it under the GPL if desired.\(^{1787}\)

The main function of the MIT license is to disclaim liability for derivative works, which allows for great flexibility in incorporating MIT-licensed code. The main benefit of using the MIT license over GPL is that it lets future programmers incorporate the MIT-licensed software into closed source programs, which can then be sold, whereas GPL requires they remain free.\(^{1788}\)

### 13.3.5 Blockchain Network Licenses

The software that runs the Ethereum network has always been available to developers and end users under the GPL.\(^{1789}\) The use of open source licensing ensures that no derivative products of the Ethereum blockchain can be later copyrighted and used for financial gain, which would be contrary to the true ethos of public blockchain technology. The Bitcoin Core software, as originally

---

\(^{1783}\) See Hoffman, supra note 1781.


released by Satoshi Nakomoto, was released under an MIT license that contains very few restrictions. Due to Nakamoto’s elusive nature, the exact reason for choosing the MIT license is unclear, but the popular presumption is that Nakamoto was aiming to retain a copyright interest in the source code.\textsuperscript{1790}

\section{13.4 DMCA}

\subsection{13.4.1 Takedown Notices and Subpoenas}

The Digital Millennium Copyright Act (DMCA), enacted in 1998, criminalizes the production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works.\textsuperscript{1791} The DMCA also increased the penalties for copyright infringement where the infringement was committed for financial gain.\textsuperscript{1792} The DMCA was initially created to implement the World Intellectual Property Organization treaties in the United States because the transition in copyrighted works from physical to electronic form demanded a shift in copyright law.\textsuperscript{1793} Today, the DMCA is used to balance the interests between copyright holders and Internet service providers (ISPs) in digital commerce.

In order to strike a balance between deterring infringement and allowing ISPs to conduct legal business operations, the DMCA contains a number of safe harbor provisions that protect parties from copyright infringement claims.\textsuperscript{1794} To rely on this protection, a party must be an Internet “service provider” (ISP) as defined under the DMCA. The DMCA covers four different categories of ISPs, all broad enough to include many organizations that likely would not consider themselves to be ISPs: transitory communications, where the provider merely transmits connections through an automatic process and acts as a conduit for data submitted by another; system caching, where the provider offers temporary storage of such material; storage of materials at the direction of a user, where the provider hosts sites or runs mailing lists; and information location tools, where the provider acts as a search engine.\textsuperscript{1795} Any company that provides these or similar services should register as a designated agent to receive notifications of claimed copyright infringement.\textsuperscript{1796} The agents are registered under the DMCA Designated Agent Directory.\textsuperscript{1797}


\textsuperscript{1791} Executive Summary, Digital Copyright Act, Section 104 Report, \url{https://www.copyright.gov/reports/studies/dmca/dmca_executive.html}.

\textsuperscript{1792} 17 U.S.C. § 506.

\textsuperscript{1793} See Executive Summary, \textit{supra} note 1791.


\textsuperscript{1795} 17 U.S.C. § 512.

\textsuperscript{1796} 17 U.S.C. § 512(c)(2); Ivan Hoffman, \textit{Are you a Service Provider} (2001), \url{http://www.ivanhoffman.com/provider.html}.

Where a copyright owner discovers infringing material on an ISP’s site, the owner has the right to send notice to the ISP’s designated agent demanding removal of the material.\(^{1798}\) If the notice is proper and the ISP promptly complies, the ISP is exempt from liability to the copyright owner and to the person who posted the material that was removed.\(^{1799}\) It is important for the owner’s notice to strictly comply with the DMCA notice requirements\(^{1800}\) as a defective notice does not allow the owner to hold the ISP liable under the DMCA if it fails to remove the infringing material.\(^{1801}\) In the event that a supposed copyright owner is abusing the notice procedure, the DMCA allows the person posting the material to file a counter-notice that requires the ISP to repost the material on its service within 10-14 days.\(^{1802}\)

If a legitimate copyright owner is subject to repeated infringements from the same party, the DMCA contains a provision allowing the owner to subpoena the identification of the infringer from the ISP.\(^{1803}\) The subpoena provision is applicable to all of the DMCA-defined categories of ISPs except transitory communications where the ISPs act as a mere conduit for information or a host for connections. In *RIAA v. Verizon*,\(^{1804}\) the RIAA sought to use the subpoena provision to force Verizon to reveal the identity of a subscriber who had allegedly used P2P software to share music online. The D.C. Circuit Court of Appeals held the DMCA does not authorize subpoenas to ISPs that merely provide Internet connections to infringers, even when subscribers use those connections to participate in P2P networks.\(^{1805}\) Judge Douglas Ginsburg opined that Congress did not foresee P2P file transmission when it drafted the DMCA, and that the DMCA was not written broadly enough to cover reach such technology.\(^{1806}\)

In light of this decision, which the U.S. Supreme Court declined to review, it appears unlikely the courts will rule that DMCA subpoenas are permissible for decentralized P2P ISPs, such as blockchain networks. Consequently, it is unlikely that blockchain P2P ISPs will ever find themselves in a position where they must jeopardize the anonymity of their users under the DMCA. Moreover, the takedown provisions of the DMCA would be difficult to enforce against blockchains given the immutability of transactions. While an ISP would certainly be able to locate the use of copyrighted material and utilize timestamps as proof of existence to assert rightful copyright where ownership is in dispute, the ISP would be unable to edit the blockchain in order to remove any infringement that was identified.

---

\(^{1798}\) 17 U.S.C. § 512(c)(3).

\(^{1799}\) 17 U.S.C. § 512(g).


\(^{1802}\) 17 U.S.C. § 512(g)(2)(C).

\(^{1803}\) 17 U.S.C. § 512(h).

\(^{1804}\) *Recording Indus. Ass’n of Am. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229 (D.C. Cir. 2003).

\(^{1805}\) *Id.* at 1236.

\(^{1806}\) *Id.* at 1238.
13.5 Trade Secrets Theft

13.5.1 Economic Espionage Act

The U.S. Economic Espionage Act of 1996 (EEA) defines a ‘trade secret’ as information that derives independent economic value – whether actual or potential – from not being generally known or readily ascertainable, and that is the subject of reasonable efforts to maintain its secrecy.\(^{1807}\) The EEA prohibits the theft of trade secrets with the knowledge or intent that the theft will injure the trade secret’s owner,\(^{1808}\) and economic espionage, which the EEA defines as the misappropriation of trade secrets with the knowledge or intent to benefit a foreign power.\(^ {1809}\) For individuals, penalties for violations of the EEA include fines of up to $5 million per offense and imprisonment for up to 15 years. For organizations, the fine is the greater of $10 million or three times the value of the stolen trade secret.\(^{1810}\)

The EEA is not intended to criminalize all thefts of trade secrets since civil remedies for that conduct typically exist under state law. The Department of Justice’s Criminal Division has issued a prosecution policy that sets forth discretionary factors for the determination of whether to indict under the EEA.\(^ {1811}\) The factors include the scope of the criminal activity, including evidence of involvement by a foreign government, the degree of economic injury caused, the type of trade secret misappropriated, the effectiveness of available civil remedies, and the potential deterrent value of the prosecution.\(^ {1812}\)

In United States v. Lange,\(^ {1813}\) the court held that the Government could only prosecute a potential defendant if the owner of the stolen trade secrets had taken reasonable measures to ensure that the information remained secret.\(^ {1814}\) In that case, a former employee had offered to sell a secret manufacturing process to his former employer’s competitor. When the former employer learned of the attempt, it reported the former employee to the FBI, which led to the employee’s being convicted and sentenced to 30 months in prison. The case was successful due largely to the reasonable measures that the former employer had taken to safeguard the secret information. The record showed that the former employee had actively sought to circumvent these measures, including physically securing the process, limiting the distribution of documentation concerning the process, limiting the number of employees with access to the process, notifying and warning

\(^{1807}\) 18 U.S.C. § 1839.

\(^{1808}\) 18 U.S.C. § 1832.


\(^{1810}\) Id.


\(^{1812}\) Id.

\(^{1813}\) United States v. Lange, 312 F.3d 263 (7th Cir. 2002).

employees they were working with confidential information, and only providing vendors with parts of the process to ensure that it could not be replicated.\textsuperscript{1815}

The U.S. Defend Trade Secrets Act (DTSA), enacted in 2016, created a federal private right of action for trade secret misappropriation.\textsuperscript{1816} The Act also amended the EEA to provide immunity to whistleblower employees for disclosure of a trade secret in confidence to an attorney or government official where the purpose is to report or investigate reports that their employers have stolen trade secrets.\textsuperscript{1817} Employers are required to include notice of this immunity in any employment agreement that governs trade secrets and other confidential information, which helps to ensure that employees do not fear retaliation when reporting violations of the DTSA.\textsuperscript{1818}

\begin{itemize}
\item\textsuperscript{1815} Lange, 312 F.3d at 266.
\item\textsuperscript{1816} 18 U.S. Code § 1836.
\item\textsuperscript{1817} 18 U.S. Code § 1833.
\item\textsuperscript{1818} Id.
\end{itemize}
Chapter 14
14 Online Gambling
14.1 Cryptocasinos

The global gambling industry has a massive net worth of over $450 billion.1819 Online gambling is a rapidly growing sector that was worth $24.73 billion in 20091820 and is predicted to exceed $60 billion by 2020.1821 A casino’s profits are typically derived from its “house edge,” which is the mathematical advantage a game provides to the house. The edge allows casinos to offer free drinks, entertainment, travel deals, and other amenities to improve the gambling experience.

Online casinos provide players with the convenience of gambling at home, yet offer a sparser experience. These casinos charge for necessities such as currency deposit, withdrawal, and exchange fees. Due to the use of third-party banks when dealing with deposits and withdrawals of fiat currency, there is usually a 2- to 3-day delay when transferring money between the online casino and the player.

Blockchain-based gambling with cryptocurrencies eliminates high bank transaction fees and money transfer delays. Cryptocasinos operate similarly to online casinos, offering similar chance- and skill-based games but accepting only virtual currency. This means any prospective player must already own the virtual currency that the particular cryptocasino accepts. There are no options to buy, sell, or exchange virtual currencies.

Cryptocurrencies, such as bitcoin and Ether, are ideal for gambling because players receive their winnings almost instantly. There are no deposits or bank wires to wait for, because the cryptocurrency transactions themselves are automatic “payment processors,” executed through executable distributed code contracts1822 (EDCC) instead of by a third-party.1823 Further, the worldwide uniformity of virtual currencies such as bitcoin and Ether enables international gambling without the need for expensive and clumsy currency exchanges.1824 Transaction costs

---


1820 Id.


1822 See Chapter 16 (Executable Distributed Code Contracts).

1823 At the time of writing, Bitcoin averages a mining time of approximately 9.22 minutes, see Blockchain, Bitcoin Stats, https://blockchain.info/stats (last visited Nov. 21, 2018), while Ethereum averages around 15 seconds; see also Ethstats, Ethereum Network Status, https://ethstats.net (last visited Nov. 21, 2018).

are negligible in comparison to the fees associated with international bank transfers and foreign currency exchange fees. Moreover, cryptocurrency transactions are irreversible, which eliminates the risk of chargeback fraud for cryptocasino operators. As a result, cryptocurrency gambling sites can offer games with a substantially lower house edge than traditional casino games. For example, traditional casino sites generally have a house edge of 3-15%, depending on the games offered, while most cryptocurrency casinos have an edge of 0.5-3%. For card games, the transparency of the blockchain also allows all players to verify that each bet is provably fair by using EDCCs containing explicit algorithms, such as the Fisher-Yates shuffle or Mersenne twister algorithm. CoinRoyale, an online bitcoin casino, uses both of these algorithms to create an initial random deck, which is then given a value in the form of a SHA-256 cryptographic hash. If the initial deck is changed in any way, the resulting hash would then be completely different, and, consequently, the game would not be verified as fair. Any player can use the blockchain to verify that the deck was not altered by taking the initial deck, dealer seed, and player seed to calculate that the hash of these inputs matches that of the final deck.

The foregoing method of independent fairness verification is unavailable to players on non-cryptographic online gambling casinos, which generally fail to state what random algorithms they use for deck shuffling. Indeed, even if non-cryptographic casinos did provide such information, players would have no way to check that the particular algorithm was being utilized. The ability

---


1826 Id.

1827 Id.


1830 The Mersenne Twister algorithm is a large linear-feedback shift register, which generates random numbers, and is considered a pseudorandom number generator. John Savard, The Mersenne Twister, http://www.quadibloc.com/crypto/co4814.htm (last visited Nov. 21, 2018).


1832 Id.

1833 Seeds are random numbers selected by the casino and player that determine the number of shuffles of a deck or rolls of a dice. See GamblingBitcoin.com, Provably Fair Bitcoin Gambling Explained, https://gamblingbitcoin.com/provably-fair/ (last visited Nov. 27, 2018); see also CoinRoyale, supra note 1831; DiceSites.com, What Is “Provably Fair”? , https://dicesites.com/provably-fair (last visited Nov. 27, 2018).
of players to confirm through the blockchain that a cryptocasino implemented a fair randomization algorithm both provides trust in the system and ensures that cryptocasinos do not exploit users by maintaining an unfairly high house edge.1834

In February 2017, a project called Edgeless Casino, designed to run on the Ethereum blockchain, launched a crowdsale with an accompanying whitepaper promising to reduce the online casino’s house edge to nearly 0% in two games, Edge Black Jack and Video Poker. In March 2017, Edgeless released a beta version of Edgeless Black Jack. When played perfectly, with the player being aware of the house edge,1835 Las Vegas-style Blackjack typically has a house edge of 0.28%. To compensate for this edge, Edgeless Casino offers incentives to the player, such as an increased blackjack payout, to reduce the house edge to 0%.1836 On December 12, 2017, Edgeless was granted a casino license in Curaçao, making it the first blockchain-based casino to be approved by legal authorities.1837 Edgeless opened to the public on January 18, 2018,1838 and offers players the option of playing blackjack, dice, baccarat or crash, while sports betting is referenced as “upcoming.”1839

14.2 State Gambling Laws

Currently, there are significant interstate restrictions on online gambling that may have consequences for cryptocasinos. While each state can regulate or prohibit the practice within its borders, only a couple have legalized online gambling, such as Nevada, Pennsylvania, Delaware, and New Jersey.1840

---

1834 D’Anconia, supra note 1825.
1836 B. Holmes, supra note 1819.
In 2011, Nevada enacted two laws\textsuperscript{1841} authorizing the Nevada Gaming Commission to license entities that conduct intrastate interactive gaming\textsuperscript{1842} and mobile gaming, respectively.\textsuperscript{1843} In December 2011, the Commission adopted certain new regulations and amendments to existing regulations\textsuperscript{1844} to implement the new laws, including requirements for operators to have effective geolocation and player authentication capabilities.\textsuperscript{1845}

Also, to protect players, operators are required to maintain cash or cash equivalents in amounts equal to the funds held in players’ accounts, and to make disclosures, such as house rules, on the operator’s website.\textsuperscript{1846} Further, regulations require operators to have internal controls to ensure security of the system and fairness of the game, such as standards for preventing collusion and protecting players’ accounts.\textsuperscript{1847} Penalties are severe as the Nevada Gaming Commission “may limit, condition, suspend, revoke or fine any license, registration finding of suitability or approval given or granted under this regulation on the same grounds as it may take such action with respect to any other license, registration, finding of suitability or approval.”\textsuperscript{1848}


\textsuperscript{1842} Nev. Rev. Stat. § 463.016425 ("'Interactive gaming' means the conduct of gambling games through the use of communications technology [including through the Internet] that allows a person, utilizing money, checks, electronic checks, electronic transfers of money, credit cards, debit cards or any other instrumentality, to transmit to a computer information to assist in the placing of a bet or wager and corresponding information related to the display of the game, game outcomes or other similar information.").

\textsuperscript{1843} Nev. Rev. Stat. § 463.0176 ("'Mobile gaming’ means the conduct of gambling games through communications devices operated solely in an establishment which holds a nonrestricted gaming license and which operates at least 100 slot machines and at least one other game by the use of communications technology that allows a person to transmit information to a computer to assist in the placing of a bet or wager and corresponding information related to the display of the game, game outcomes or other similar information. For the purposes of this section, ‘communications technology’ means any method used and the components employed by an establishment to facilitate the transmission of information, including, without limitation, transmission and reception by systems based on wireless network, wireless fidelity, wire, cable, radio, microwave, light, optics or computer data networks. The term does not include the Internet.").

\textsuperscript{1844} Nev. Gaming Comm’n Regs. 3, 4, 5, 5A, 8, 14, 15, 15A, 15B.

\textsuperscript{1845} Nev. Gaming Comm’n Regs. §§ 5A.110(5), 5A.120(1)(c).

\textsuperscript{1846} Nev. Gaming Comm’n Regs. §§ 5A.125, 5A.150.

\textsuperscript{1847} Nev. Gaming Comm’n Regs. § 5A.070.

\textsuperscript{1848} Nev. Gaming Comm’n Reg. §5A.200(2).
Subsequently, Delaware, Pennsylvania, and New Jersey followed suit, imposing similar requirements for licensing, geolocation, and player authorization. By contrast, other states that have either banned online gambling specifically (e.g., Montana, which defines “illegal gambling enterprise” to include “internet gambling,” and Illinois, which penalizes operators of

\[1849\] Del. Code Ann. tit. 29, § 4803(k) ("'Internet lottery' shall mean all lottery games in which the player's interaction with the game operated by the Office occurs over the Internet (which, for purposes of this chapter, shall include any public or private computer or terminal network, whether linked electronically, wirelessly, through optical networking technology or other means), including Internet ticket games, the Internet video lottery and Internet table games”); Del. Code Ann. tit. 29, § 4826; 10-200-206 Del. Code Regs. § 13.1-13.9; 10-200-206 Del. Code Regs. § 13.22.

\[1850\] 4 Pa. C.S. § 502 ("'iLottery Game.' Internet instant games and other lottery products offered through iLottery. The term does not include games that represent physical, Internet-based or monitor-based interactive lottery games which simulate casino-style lottery games, specifically including poker, roulette, slot machines or blackjack"); 4 Pa. C.S. § 502 ("'Internet Instant Game.' A lottery game of chance in which, by the use of a computer, tablet computer or other mobile device, a player purchases a lottery play, with the result of play being a reveal on the device of numbers, letters or symbols indicating whether a lottery prize has been won according to an established methodology as provided by the lottery"; 4 Pa. C.S. § 13C01 ("'Sports Wagering.' The business of accepting wagers on sporting events or on the individual performance statistics of athletes in a sporting event or combination of sporting events by any system to method of wagering, including over the Internet through websites and mobile applications. The term includes, but is not limited to, exchange wagering, parleys, over-under, money line, pools and straight bets…")

\[1851\] N.J. Stat. Ann. § 5:12-28.1 ("'Internet gaming’ means the placing of wagers with a casino licensee at a casino located in Atlantic City using a computer network of both federal and non-federal interoperable packet switched data networks through which the casino licensee may offer authorized games to individuals who have established a wagering account with the casino licensee and who are physically present in this State, as authorized by rules established by the division.”); N.J. Stat. Ann. § 5:12-5 ("'Authorized Game’ or ‘Authorized Gambling Game’—Roulette, baccarat, blackjack, craps, big six wheel, slot machines, mini baccarat, red dog, paigow, and sic bo; any variations or composites of such games, provided that such variations or composites are found by the division suitable for use after an appropriate test or experimental period under such terms and conditions as the division may deem appropriate; and any other game which is determined by the division to be compatible with the public interest and to be suitable for casino use after such appropriate test or experimental period as the division may deem appropriate. ‘Authorized game’ or ‘authorized gambling game’ includes gaming tournaments in which players compete against one another in one or more of the games authorized herein or by the division or in approved variations or composites thereof if the tournaments are authorized by the division.”); N.J. Admin. Code § 13:69O-1.2(e); N.J. Admin. Code § 13:69O-1.3(b).

\[1852\] Mont. Code Ann. § 23-5-112 ("'Internet gambling’, by whatever name known, includes but is not limited to the conduct of any legal or illegal gambling enterprise through the use of communications technology that allows a person using money, paper checks, electronic checks,
internet gambling sites\textsuperscript{1853}) or prohibited gambling in general regardless of where a player is located (e.g., New York,\textsuperscript{1854} which prohibits the promotion of gambling\textsuperscript{1855} and the possession of gambling devices).\textsuperscript{1856}

As gambling in cryptocasinos entails sending wagers over the Internet using a computer network, cryptocasinos fall within the scope of Nevada, Delaware, Pennsylvania and New Jersey’s respective Internet gambling statutes. Accordingly, cryptocasinos operating in these states would be obligated to comply with the same regulations as online casinos, including obtaining a license, having geolocation capabilities on their platforms, and maintaining internal controls to verify players. For example, in 2015, Seals with Clubs, an online gaming site that accepted wagers in the form of bitcoin, ceased operations, and its operator, Bryan Micon, pleaded guilty to operating an unlicensed interactive gaming website in violation of Nevada law.\textsuperscript{1857}

---

\textsuperscript{1853} 720 Ill. Comp. Stat. Ann. 5/28-1 (“A person commits gambling when he or she: … (12) knowingly establishes, maintains, or operates an Internet site that permits a person to play a game of chance or skill for money or other thing of value by means of the Internet or to make a wager upon the result of any game, contest, political nomination, appointment, or election by means of the Internet. This item (12) does not apply to activities referenced in items (6) and (6.1) of subsection (b) of this Section.”).

\textsuperscript{1854} N.Y. Penal Law § 225.00, et seq.; People ex rel. Vacco v. World Interactive Gaming Corp., 185 Misc. 2d 852, 859–60, 714 N.Y.S.2d 844, 850 (Sup. Ct. 1999) (“The act of entering the bet and transmitting the information from New York via the Internet is adequate to constitute gambling activity within the New York state.”).

\textsuperscript{1855} N.Y. Penal Law § 225.00(2), (6) (“‘Gambling.’ A person engages in gambling when he stakes or risks something of value upon the outcome of a contest of chance or a future contingent event not under his control or influence, upon an agreement or understanding that he will receive something of value in the event of a certain outcome;” “‘Something of value’ means any money or property, any token, object or article exchangeable for money or property, or any form of credit or promise directly or indirectly contemplating transfer of money or property or of any interest therein, or involving extension of a service, entertainment or a privilege of playing at a game or scheme without charge.”).

\textsuperscript{1856} N.Y. Penal Law § 225.00(7) (“‘Gambling device’ means any device, machine, paraphernalia or equipment which is used or usable in the playing phases of any gambling activity, whether such activity consists of gambling between persons or gambling by a person involving the playing of a machine. Notwithstanding the foregoing, lottery tickets, policy slips and other items used in the playing phases of lottery and policy schemes are not gambling devices.”).

14.3 Federal Law

By operating interstate, cryptocasinos may also run afoul of certain federal laws, such as the Wire Act of 1961, the Travel Act of 1961, the Illegal Gambling Business Act of 1970, and the Unlawful Internet Gambling Enforcement Act of 2006. The statutory language of these acts does not expressly prohibit online gambling, yet courts and the Department of Justice have interpreted them as such.

The Wire Act prohibits gambling businesses from using wire communication facilities for interstate and foreign transmissions of bets and wagers. Federal courts have held that the Internet is a wire communication facility, meaning online bets and wagers would fall within the scope of the statute. Additionally, the Wire Act reaches beyond the United States to apply to any international company taking online sports bets from U.S. citizens. Courts are, however, split as to whether the Wire Act applies only to sports betting or whether its prohibition extends to games of chance as well. In 2011, the Department of Justice’s Office of Legal Counsel, which provides written opinions to various executive branch agencies and offices within the Department of Justice, opined that the Wire Act only applied to transmissions of wire communications that

---

1862 18 U.S.C. § 1084 (“Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined under this title or imprisoned not more than two years, or both.”).
1863 United States v. Cohen, 260 F.3d 68, 76 (2d Cir. 2001); United States v. Lyons, 740 F.3d 702, 716 (1st Cir. 2014) (noting “the internet is used and useful in the transmission of writings”).
1864 18 U.S.C.A. § 1081 (“The term ‘wire communication facility’ means any and all instrumentalities, personnel, and services (among other things, the receipt, forwarding, or delivery of communications) used or useful in the transmission of writings, signs, pictures, and sounds of all kinds by aid of wire, cable, or other like connection between the points of origin and reception of such transmission.”).
1865 United States v. Lyons, 740 F.3d at718.
1866 Compare In re MasterCard Int'l Inc., Internet Gambling Litig., 132 F. Supp. 2d 468, 480 (E.D. La. 2001), aff’d sub nom. In re MasterCard Int'l Inc., 313 F.3d 257 (5th Cir. 2002), with United States v. Lombardo, 639 F. Supp. 2d 1271, 1281 (D. Utah 2007) (concluding “that § 1084(a) is not confined entirely to wire communications related to sports betting or wagering.”).
relate to sporting events or contests. Thus, cryptocasinos offering sports betting (or even blockchain-based predictive markets that wager on the outcome of sporting events) across state or international boundaries likely violate the Wire Act.

The Travel Act prohibits the use of U.S. mail, or any facility in interstate or foreign commerce, with the intent to distribute proceeds of any unlawful activity, which includes any business enterprise involving gambling in violation of state law. Physical travel is not required since the use of the Internet qualifies as an interstate facility even if the facility was used wholly intrastate. Thus, a cryptocasino operating solely in Nevada, Delaware, Pennsylvania, or New Jersey in compliance with all applicable laws in those states might be safe from prosecution, but a cryptocasino operating in a state that does not permit online gambling would violate the Travel Act.

The Illegal Gambling Business Act (IGBA) prohibits the conduct, financing, management, supervision, direction, and ownership of an illegal gambling organization, which is defined as a gambling business that violates state or local law, involves five or more people who provide “necessary and useful functions,” and either has been in “substantially continuous operation” for more than 30 days or accumulates $2,000 in gross revenue in a single day.


1868 18 U.S.C. § 1952. Penalties vary depending upon the particular Travel Act violation, such as fine or imprisonment of not more than 5 years, or both, for violations that involve the intent to promote or distribute proceeds of an unlawful activity, or a fine or imprisonment of not more than 20 years, or both, for violations that involve an intent to commit a violent crime to further an unlawful activity. 18 U.S.C. § 1952(a)(3)(A), (B).


1870 United States v. Nader, 542 F.3d 713, 716 (9th Cir. 2008) (noting “intrastate telephone calls made with intent to further unlawful activity can violate the Travel Act”).

1871 United States v. Trupiano, 11 F.3d 769, 773-74 (8th Cir. 1993) (holding that “substantially continuous operation” requires some “schedule of regularity,” and does not “mean every day”).

1872 United States v. DiMuro, 540 F.2d 503, 508 (1st Cir. 1976) (concluding that persons who helped transmit gambling information were “engaged in ‘an illegal gambling business’”).

1873 United States v. Trupiano, 11 F.3d 769, 773-74 (8th Cir. 1993) (holding that “substantially continuous operation” requires some “schedule of regularity,” and does not “mean every day”).

1874 18 U.S.C. § 1955. Whoever violates the IGBA is subject to a fine or imprisonment of not more than five years, or both.
The government must prove that the defendant and at least four others were involved in the gambling business itself, though “the jurisdictional five persons may include unindicted and unnamed persons.”\textsuperscript{1875} Additionally, the government does not need to prove that the five individuals that were involved for the statutory 30-day period were the same individuals involved for the entire duration of the operation.\textsuperscript{1876} Accordingly, anyone – including an owner, accountant, computer operator, or computer maintenance person\textsuperscript{1877} – who is necessary and useful for the operation of a cryptocasino in a state that prohibits gambling may be prosecuted under the IGBA, if the cryptocasino has been operating for more than 30 days or receives more than $2,000 in gross revenue in a single day.

The Unlawful Internet Gambling Enforcement Act\textsuperscript{1878} (UIGEA) prohibits businesses engaged in betting and wagering\textsuperscript{1879} from knowingly accepting credit,\textsuperscript{1880} electronic funds transfers or funds transmitted by a money transmitting business,\textsuperscript{1881} any check,\textsuperscript{1882} or the proceeds of any other financial transaction as prescribed by regulation,\textsuperscript{1883} in connection with a person’s participation in unlawful Internet gambling.\textsuperscript{1884} Thus, a gambling business violates the UIGEA if

\begin{itemize}
  \item[\textsuperscript{1875}] United States v. Trupiano, 11 F.3d 769, 772-73 (8th Cir. 1993).
  \item[\textsuperscript{1876}] United States v. Murray, 928 F.2d 1242, 1246 (1st Cir. 1991).
  \item[\textsuperscript{1877}] Seth Gorman & Anthony Loo, Blackjack or Bust: Can U.S. Law Stop Internet Gambling, 16 Loy. L.A. Ent. L. Rev. 667, 676 (1996).
  \item[\textsuperscript{1878}] 31 U.S.C. § 5363.
  \item[\textsuperscript{1879}] ‘Bet or wager’ “means the staking or risking by any person of something of value upon the outcome of a contest of others, a sporting event, or a game subject to chance, upon an agreement or understanding that the person or another person will receive something of value in the event of a certain outcome.” 31 U.S.C. § 5362(1)(A).
  \item[\textsuperscript{1880}] ‘Credit’ means “the right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment.” 31 U.S.C. § 5362(11)(a); 15 U.S.C. § 1602(f).
  \item[\textsuperscript{1881}] A ‘money transmitting business’ is generally a business that “provides check cashing, currency exchange, or money transmitting or remittance services, or issues or redeems money orders, travelers' checks, and other similar instruments or any other person who engages as a business in the transmission of funds.” 31 U.S.C. § 5362(11)(e); 31 U.S.C. § 5330(d)(1). ‘Money transmitting service’ “includes accepting currency or funds denominated in the currency of any country and transmitting the currency or funds, or the value of the currency or funds, by any means through a financial agency or institution.” 31 U.S.C. § 5330(d)(2).
  \item[\textsuperscript{1882}] 31 U.S.C. § 5363.
  \item[\textsuperscript{1883}] ‘Restricted transactions’ means transactions or transmittals involving credit, an electronic funds transfer or funds transmitted by a money transmitting business, and checks. 12 C.F.R. § 233.2(y).
  \item[\textsuperscript{1884}] “The term ‘unlawful internet gambling’ means to place, receive, or otherwise knowingly transmit a bet or wager by any means which involves the use, at least in part, of the Internet where such bet or wager is unlawful under any applicable Federal or State law in the State or Tribal lands in which the bet or wager is initiated, received, or otherwise made.” 31 U.S.C. § 5362(10)(a).
\end{itemize}
it accepts funds from a person engaged in online gambling when such activity is unlawful in the state where the bet or wager is initiated or received.\textsuperscript{1885}

A cryptocasino could fall within the ambit of the UIGEA. The Treasury Department and the Federal Reserve have yet to prescribe any other financial transaction pursuant to Section 5363(4), and virtual currency does not seem to fit the definitions of “credit” or “check.” However, virtual currency exchanges could still qualify as “money transmitting businesses,” as defined under Section 5362(11)(e), because the exchanges accept currency and transmit the value of such currency (in the form of virtual currency) through a financial agency or institution.\textsuperscript{1886} Thus, if a cryptocasino accepts funds transmitted from a virtual currency exchange, and the online bet or wager is unlawful in the state where it is initiated (i.e., where the player is located) or received (i.e., where the cryptocasino is located), then the cryptocasino could be prosecuted under the UIGEA.

The passage of the UIGEA in 2006 led many foreign gambling sites to discontinue accepting players from the United States, and the ripple effects from the passage of the Act caused massive declines in stock value for the companies affected.\textsuperscript{1887} Party Gaming,\textsuperscript{1888} an online gambling company, attempted to remain in the U.S. market, but its publicly traded stock dropped almost 60\% in value within 24 hours of the bill’s passage.\textsuperscript{1889} Party Gaming swiftly pulled out of the U.S. market later that year along with several other poker sites.\textsuperscript{1890} Five years after the passage of the Act, in April 2011, the Department of Justice unsealed a 52-page indictment against top executives of the three largest online poker companies, PokerStars, Full Tilt Poker, and Absolute Poker, along with a $3 billion civil complaint.\textsuperscript{1891} The companies’ assets and website addresses were frozen until they agreed to shut out U.S. players.\textsuperscript{1892}

### 14.4 Lottery

Due to UIGEA, many cryptocasinos, such as SatoshiDice and Bwin, have closed their operation to U.S.-based IP addresses. SatoshiDice stated that its action was because “the courts have not been clear on the definition of gambling, nor on what would constitute ‘legitimate gaming’, nor are jurisdictions properly defined, and thus this is a proactive measure to protect

---

\textsuperscript{1885} The UIGEA excludes bets and wagers that are initiated and received within a single state. 31 U.S.C. § 5362(10)(b)(i).

\textsuperscript{1886} 31 U.S.C. § 5362(4).


\textsuperscript{1888} Party Gaming claimed that it had a 41\% share of the worldwide online poker revenue in 2006, with 77\% of that revenue from U.S. customers. GamblingSites.com History of Party Gaming, [https://www.gamblingsites.com/history/partygaming/](https://www.gamblingsites.com/history/partygaming/) (last visited Nov. 21, 2018).

\textsuperscript{1889} Gambling.com, \textit{supra} note 1887.

\textsuperscript{1890} \textit{Id.}


those involved in the project.” However, some cryptocasinos, such as Bovada and VegasCasino, do offer services to U.S. IP addresses. Thus far, no cryptocasino has faced prosecution for accepting restricted transactions under the UIGEA. Until that happens, cryptocasinos will likely continue to operate despite the legal risk.

Forty-four states and the District of Columbia, Puerto Rico, and the U.S. Virgin Islands permit lotteries. Only five states – Alabama, Alaska, Hawaii, Nevada and Utah – have no state-run lottery. Alabama and Utah cite religious objections, while Alaska and Hawaii have not felt the pressure of losing lottery sales to neighboring competing states as they are outside the contiguous United States. Nevada’s gambling industry lobbied against a state lottery, likely fearing the competition.

Despite the opposition in these five states, some lawmakers are nevertheless pushing to legalize state lotteries as a remedy for budget shortfalls. For example, on August 31, 2018, Mississippi passed SB 2001, authorizing a state lottery which proponents claim will raise $80 million for the state. Indeed, state-run lotteries can raise significant revenue, often for specific beneficiaries, such as K-12 education.

Federal statutes prohibit the mailing or transportation in interstate/foreign commerce of promotions for lotteries, or the sending of the lottery tickets themselves. A number of states have enacted provisions designed to help problem gamblers. In Louisiana, for example, all lottery tickets must be printed with a toll-free gambler’s assistance hotline phone number. One interesting provision in many state lottery laws provides for the garnishment of prizes to collect

---

1897 Id.
1898 Id.
1899 Id.
1902 Wagster, supra note 1900.
1903 18 U.S.C § 1301.
various debts, ranging from unpaid taxes to outstanding child support obligations.\textsuperscript{1905}

Lotteries are the most popular form of gambling in the developed world, with over 50\% of citizens in industrialized nations playing a lottery regularly.\textsuperscript{1906} Blockchain technology is currently being developed to bring transparency to lotteries, such as the Ethereum-based application KIBO, with the purpose of solving common problems, including fair drawings, collection of winnings, and limited access to ticket purchases.\textsuperscript{1907}

The logic and algorithms of executable distributed code contracts (EDCCs) and blockchain technology would be accessible to anybody, meaning any individual could confirm a transaction, draw, or lottery. This ensures complete transparency and almost 100\% fair play. KIBO uses Ether, which allows the lottery to be accessed any place in the world via an Internet connection, unlike traditional lotteries, which are restricted by geographical location.\textsuperscript{1908} Additionally, in traditional lotteries, it can often take months or even years for winners to receive their prize money, whereas blockchain-based lotteries could distribute winnings automatically, with no transaction or distribution fees.

\textbf{14.5 Sports Betting}

In addition to the above-mentioned federal laws, sports betting was regulated by the Professional and Amateur Sports Protection Act (PAPSA).\textsuperscript{1909} Congress passed PAPSA in 1992 in response to growing concerns over state-sponsored sports gambling. PAPSA preempted state law and made it illegal for any government agency or private person to “sponsor, operate, advertise, or promote” a scheme based on “one or more competitive games in which amateur or professional athletes participate…”\textsuperscript{1910} PAPSA did not make sports gambling a federal crime; rather, it allowed the Attorney General, as well as professional and amateur sports organizations, to bring civil actions to enjoin possible violations of the law.\textsuperscript{1911} PAPSA included a grandfather clause that exempted states which already had laws permitting sports betting on the books, including Nevada, Oregon, Delaware and Montana.\textsuperscript{1912}

In October 2016, the State of New Jersey filed a petition for a writ of \textit{certiorari} to the Supreme Court, \textit{Murphy v. NCAA}, with the question being: “Does a federal statute that prohibits modification or repeal of state-law prohibitions on private conduct impermissibly commandeer the

\textsuperscript{1905} Tex. Govt. Code § 466.4075.


\textsuperscript{1907} \textit{Why KIBO Lotto?}, \texttt{https://kiboplatform.net/en/advantages.html} (last visited Nov. 21, 2018).

\textsuperscript{1908} \textit{Id}.

\textsuperscript{1909} 28 U.S.C. § 3702.

\textsuperscript{1910} \textit{Id}.

\textsuperscript{1911} 28 U.S.C. § 3702(1).

\textsuperscript{1912} 28 U.S.C. § 3704.
regulatory power of the States?" After granting the petition and receiving briefing and hearing arguments, the Supreme Court ruled on May 14, 2018 that PAPSA is unconstitutional because it violates the anti-commandeering provisions inherent in the Tenth Amendment. As a result, states are no longer prohibited from authorizing and regulating sports wagering systems. States that wish to permit sports betting within their states can now pass legislation and adopt appropriate regulations. New Jersey, Pennsylvania, Mississippi and West Virginia have all recently passed bills to legalize sports betting.

Several blockchain companies are now providing individuals with the ability to place sports bets directly on the blockchain. In September 2018, Wagerr, which operates on a single service blockchain, announced that after private and public testing, it was releasing its Wagerr Betting platform. To participate in Wagerr’s platform, individuals have three options: (1) placing sports bets; (2) becoming the operator of an Oracle Masternode; or (3) holding Wagerr coin (WGR) as an investment. Wagerr uses Application-Specific Smart Contracts, which are single-purpose blockchain smart contracts that only accept fixed parameters. The platform also implements “Direct-Chain” betting, where users can place bets against the chain itself, and the chain will mint coins to pay winners as required. The Direct-Chain betting fee is 6% of the profit from the winning bets, a portion of which is distributed to all active Oracle Masternodes. Wagerr’s first betting event took place on September 15, 2018 for the Canelo v. GGG 2 boxing match, which the company reported “flawless release.” In 2019, Wagerr plans to incorporate fantasy sports and live betting into its platform.

---

1914 Id. at 1476-1481.
1919 An oracle acts as a consensus agent that retrieves real-world sporting event data and records the outcomes on the blockchain. The information is then used by the network to determine winning bets. The oracles also act as masternodes in that they exclusively initiate the betting of smart contracts backed by their collateral thereby forming a strong and reliable second tier network. Wagerr: Oracle, https://www.wagerr.com/oracles (last visited Dec. 17, 2018).
14.6 Prediction Markets

Prediction markets are exchange-traded markets created by individuals on market-hosting websites to trade in the outcomes of future events, with market prices reflecting what bettors believe is the probability of the posited event.\(^{1924}\) Prediction markets are generally quite successful at predicting future outcomes for three key reasons: (1) those who make accurate predictions receive financial benefits, while those who make bad predictions suffer losses, discouraging the latter from participating over time; (2) prediction markets are democratic, allowing large groups of people from diverse perspectives to participate, thereby negating participants’ individual biases; and (3) people who place bids early and furthest from conventional wisdom receive the biggest rewards, incentivizing people to consider unlikely outcomes and avoid erroneous groupthink.\(^{1925}\)

Most prediction markets that operate online and use fiat currency are often considered online gambling, rendering them illegal in most jurisdictions. However, there are at least two legal markets, PredictIt\(^{1926}\) and the Iowa Electronic Markets,\(^{1927}\) each of which is a nonprofit research project partnered with a university. A for-profit predictive market in Ireland, Intrade, was sued in 2012 by the Commodity Futures Trading Commission for accepting payment from Americans in violation of the Commodity Exchange Act.\(^{1928}\) PredictIt and Iowa Electronic Markets both gained approval from the CTFC before trading in the United States and secured a “no action” letter to ensure they were operating free of the possibility of prosecution.\(^{1929}\)

14.6.1 Augur and Gnosis

Two decentralized applications, Augur and Gnosis, plan to operate decentralized prediction markets built on the Ethereum blockchain. These projects seek to leverage the open peer-to-peer functionality of the blockchain, as well as game theory and financial incentives, to utilize the


\(^{1926}\) PredictIt is a project of Victoria University of Wellington, New Zealand. PredictIt, https://www.predictit.org (last visited Nov. 21, 2018).

\(^{1927}\) Iowa Electronics Market is a project of the University of Iowa. Iowa Electronics Market, http://tippie.biz.uiowa.edu/iem/ (last visited Nov. 21, 2018).


“wisdom of the crowd” for making accurate predictions of future events. Augur conducted an initial currency offering (ICO) in September 2015, raising $5.2 million worth of tokens.1930 Augur went live in July of 2018 highlighting use cases in political forecasting, weather prediction, event hedging and company forecasting.1931 In April 2017, Gnosis raised $312.8 million worth of tokens in the first 12 minutes of its ICO.1932 Gnosis has been running the alpha version of its software on the Ethereum blockchain since December 2017 but has not made any further announcements.1933

To decide whether or not a prediction came true, Augur and Gnosis have designated users called “oracles” who vote on the outcome, thereby determining winners and losers.1934 A prediction market depends on the accuracy of its oracles because, if the system is perceived as unfair or unreliable, the market loses its integrity.1935 Augur holds oracles accountable for any inaccuracies by linking their voting clout to their historical fidelity to the consensus, which allows egregious liars who repeatedly stray from consensus to be flagged by their voting patterns and stripped of their clout or removed from the system entirely.1936 Gnosis intends to utilize different types of oracles: a centralized oracle (i.e., a “single source of truth”) for most instances, and a decentralized “Ultimate Oracle” (basically, a consensus vote by all ether holders) to decide disputes when a party challenges an outcome.1937

Centralized online prediction markets are easy to manipulate and falsify, and are subject to bribery. Relying on specific individuals or programs leads to fallibility, thus destroying confidence in the system. The decentralized consensus systems used in Augur and Gnosis make it much more difficult for any one person or group to undermine the market, thus providing a perceivably fair and trustworthy platform.

---

1933 Gnosis, Gnosis Timeline https://gnosis.pm/timeline (last visited Nov. 21, 2018).
1936 Id.
Chapter 15
15 Elections

Online voting systems have the potential to make voting easier and far more accessible. Remote online voting would undoubtedly facilitate greater participation in democracy at both the national and local levels. As of January 2018, for example, 77% of Americans owned smartphones, 73% American adults owned a desktop or laptop computer, and roughly 53% of the country’s population owned tablets. If online voting were available via these devices, a greater number of Americans – likely much greater than the 59.7% of registered voters who voted in the 2016 presidential election – would participate.

Given the inconvenience and limited accessibility of polling places, which generally only operate for a single day and give rise to long lines, online voting should be a high priority for any democratic government. Yet concerns over security and transparency currently undermine any prospect of legitimacy and trust in electronic voting. Further, centralized methods for creating a "transparent" online voting system that have been discussed and proposed are generally costly and difficult to implement on a large scale. For the problems of voter fraud, transparency, cost, and administrative concerns, blockchain technology offers a solution.

---

15.1 Use of Blockchain Technology for Elections

15.1.1 Voter Registration Database

To cast a vote, a voter must first be registered. Generally, a voter may register in person at a registration site, by mail, or concurrently with an application for a driver’s license. Many states, such as California and Massachusetts, permit voters to register online. Once registered, a voter is added to a “voter list” or “voter roll,” which determines who is allowed to vote. Pursuant to the Help America Vote Act of 2002, each state must maintain this voter list on a centralized server. Having one server, however, poses security risks as the server presents a single point of failure. Critics of online voter registration systems have suggested a return to paper, but this option is cumbersome and still risks fraud and errors as paper records can be altered without evidence of tampering.

Decentralized blockchain technology, which is transparent and tamper-proof, does not suffer from these flaws. With voting lists stored on each node of the decentralized network, there is no centralized target for hackers. However, as the Help America Vote Act requires states to have “a single, uniform, official, centralized, interactive computerized statewide voter registration list,” using a blockchain to store official voting records would require the statute to be amended.

15.1.2 Proposals for Authenticating Voters and Their Votes

Beyond maintaining voter registration data, blockchain technology also provides an attractive method for recording votes. First, the ledger is transparent to all users of the blockchain, and the entire record of transactions is available to the public. This fundamental aspect of the

---

1944 Id.
1947 52 U.S.C. § 21083(a)(1)(A)(i) (“The computerized list shall serve as the single system for storing and managing the official list of registered voters throughout the State.”).
1949 Jeff Kaplan, Want Tamper-proof Elections? Start with Blockchain for Voter Registration, HuffPost (Jan. 17, 2017), http://www.huffingtonpost.com/entry/want-tamper-proof-elections-start-with-blockchain_us_5866c485e4b04d7df167d483 (“How do you know if all of the original paper records are still there? How do you know if extra records have been added? Or if some were tampered with? Paper provides no automatic alarm or auditable log of activities.”).
1951 See Chapter 2 (Blockchain Technology).
Technology should give voters faith in the system’s integrity because it can be audited and verified in real time by a decentralized mass of users.\(^{1952}\)

To implement this concept, a current proposal calls for a centralized organization that maintains the voter list, which contains a hashed code used by the voter upon registration, and a trusted third-party (TTP) that coordinates voter verification.\(^{1953}\) To vote, the individual sends to the TTP the hashed code used when he or she registered to vote, which the TTP then forwards to the centralized organization.\(^{1954}\) The centralized organization confirms whether the hashed code matches an identity someone on the voter list.\(^{1955}\) If so, the centralized organization responds affirmatively to the TTP, which records the voter’s public address and asks the voter to cast a vote. The voter then votes by sending a transaction to a candidate’s public address.\(^{1956}\)

The TTP determines the results of the election by reviewing the blockchain and filtering out any voters’ public addresses that were not approved to vote.\(^{1957}\) In the filtering process, if a voter’s public address appears multiple times (suggesting multiple votes) for a candidate, then only one vote will be counted.\(^{1958}\) Also, if a voter votes multiple times for different candidates, all of that voter’s votes will be invalidated.\(^{1959}\) For transparency, the TTP publishes the roster of votes cast and the public addresses entitled to vote (randomly listed so that the votes cast cannot be matched with public addresses), and the centralized organization publishes the voters’ identities.\(^{1960}\)

Another proposal utilizes two separate blockchains, one for recording voter registrations (and whether a particular voter has voted) and another for casting votes.\(^{1961}\) An individual registers to vote by providing identification information through a government website or by mail, and that information is sent as a transaction to the voter registration blockchain to verify whether the individual has already registered.\(^{1962}\) If the individual is not already registered, then he or she is sent a ballot card (containing a QR code) and a randomly generated password for use when voting.\(^{1963}\)

\(^{1952}\) Id.

\(^{1953}\) Lee, supra note 1942 at 126-127.

\(^{1954}\) Id. at 127.

\(^{1955}\) Id.

\(^{1956}\) Id. at 127-128.

\(^{1957}\) Id. at 131.

\(^{1958}\) Id.

\(^{1959}\) Id.

\(^{1960}\) Id.


\(^{1962}\) Id. at 8.

\(^{1963}\) Id. at 11.
Under this proposal, the voting mechanism is structured into three tiers – a local polling place tier of nodes, which are grouped and connected to intermediary nodes, which in turn are grouped and connected to national nodes, which mine transactions and add blocks to the blockchain. Voters cast their votes through local polling place nodes, which consult with the voter registration blockchain to determine if each voter has already cast a vote in that election. If the voter has not, then the local polling place node allows that voter to do so. The local polling place node then encrypts the vote using a public key provided by the intermediary node and sends the encrypted transaction to the intermediary node, which groups the transactions into blocks and pushes them to all other intermediary nodes for recording on the voting blockchain.

Once a voter has voted, the local polling place node sends a transaction to the voter registration blockchain, updating it to reflect that the voter has cast a vote. When the voting deadline has passed, an executable distributed code contract in the software of each intermediary node publishes the node’s private key, which then decrypts the voting data on the voting blockchain.

15.1.3 Blockchain Voting DApps

Several companies and countries are exploring and developing DApps to provide blockchain-based voting platforms.

Follow My Vote, which released its alpha version in August 2016, is developing a voting platform called Voting Booth, built on the Graphene blockchain. Users install Voting Booth on their computers or smartphones, and the software creates a unique private key and public key for each user. Users then enter personal identifying information into Voting Booth, which transmits it along with each person’s public key to an Identity Verifier – i.e., a person or entity,

1964 *Id.* at 9-10.
1965 *Id.* at 11.
1966 *Id.*
1967 As different groups of local polling place nodes are connected to different intermediary nodes, and as each intermediary node has a different public key, the voting transaction data sent from one group of local polling place nodes will be encrypted differently from another group. This decreases the risk that a single person will be able to decrypt all of the voting data before the voting deadline.
1969 *Id.* at 12.
1970 *Id.* at 10-11.
such as a political party, approved by the organization hosting the election to verify voters. The Identity Verifier confirms that each user has not already registered then certifies each voter for the correct ballot in Voting Booth.

The voter requests a ballot by sending the voter’s public key and a blinded token to a Registrar, an entity that issues the ballots for each voter. The Registrar signs the blinded token and returns it to the voter’s Voting Booth, which generates another set of private and public keys. Voting Booth sends the signed unblinded token and the second public key to the Registrar, who certifies the second public key for a certain ballot type, which Voting Booth then generates for the voter.

The voter actually votes by completing the ballot and submitting it to a blockchain-based ballot box. If the laws of the jurisdiction permit the voter to change a vote, only the last vote will count. The voter may also audit the ballot box to ensure that the vote was cast as intended and counted, and to confirm that the ballots in the box match the totals reported by the FMV system, without revealing the identities of the voters.


1975 Blinded tokens, also called “blind signatures,” are used to send messages anonymously. Cryptographer David Chaum, creator of the blind token method, compared it to a paper voting method where a voter places a completed ballot slip in a carbon-lined envelope, which is placed in a pre-addressed envelope showing the voter’s identity and address, which is then mailed to a trustee. The trustee signs the outside of the carbon-lined envelope, imprinting the trustee’s signature onto the ballot, and sends the carbon-lined envelope back to the voter. The voter removes the ballot, which has the trustee’s signature, and sends it to the trustee in an envelope that does not identify the voter. David Chaum, Blind Signatures for Untraceable Payments, in Advances in Cryptology: Proceedings of Crypto 82 199 (1983).


Another example of a blockchain-based voting system is Australia Post, a government-owned corporation. Once a user is verified through Australia Post’s digital identity product, the system generates digital access keys for the user as well as “voting credits” for casting votes. A ballot is represented cryptographically on the blockchain. Once the election deadline passes, the system compiles the results.

Still another example is NASDAQ Inc.’s blockchain-based proxy voting system for companies listed on the Tallinn Stock Exchange in Estonia, which successfully completed a test run in January 2017. Investors were able to vote online during investor meetings and to transfer their voting rights to a proxy. The test aimed to show that blockchain technology could reduce the complexity and cost of organizing shareholder votes, while increasing overall shareholder participation in corporate governance. The system authenticated the identities of investors through government-issued identification cards and a system-generated PIN. Overall participation was shown to increase as a result of the test, though participants requested a more user-friendly dedicated mobile application.

Other companies working in the private sector to develop blockchain-based voting systems include Agora, Blockchain Technologies Corp., and e-Vox. In the public sector, various governments have also expressed interest in utilizing blockchain technology for elections and other voting processes.

---


1981 Australia Post, supra note 1979 at 3.


1983 Id.

1984 Id.

1985 Id.

1986 Id.


In February 2016, for example, various Ukrainian government officials, responding to complaints of fraud and corruption in elections held in 2014, signed a memorandum calling for the use of e-Vox’s blockchain-based platform for elections, petitions, and local council processes. The city of Zug, Switzerland, intends to conduct an electronic vote in 2018, with voters’ identities being verified by a DApp that secures personal information on a blockchain. Additionally, in March 2017, local officials in Gyeonggi-do, South Korea used blockchain technology to conduct a vote on fund allocation for community projects. On December 4, 2017, the Moscow government announced a pilot program to migrate its Active Citizen voting system to the blockchain. The system is a private platform based on Ethereum’s open source code and governed by a Proof-of-Authority consensus mechanism. Since its December of 2017 launch, the platform has been downloaded by 100 operators. Perhaps the most notable blockchain election advance occurred on March 7, 2018, when 70% of the citizens of Sierra Leone voted using a blockchain-based platform developed by Agora, which claims it is the “only company in the world that has built a fully-functional blockchain voting platform.”

Testing of blockchain-based voting platforms has also begun in the United States. In March 2016, Utah’s Republican Party experimented with blockchain technology to conduct its caucus for presidential candidates. Users had to pre-register, and their identities were verified by the

---


party. Users were then given encrypted ID numbers to vote. Prior to the experiment, critics were concerned about the security risks of online voting, such as malware on a user’s personal device. Following the caucus, however, no security concerns were identified and accuracy of the results was not challenged.

In April 2016, the Libertarian parties in Texas and New York used Blockchain Technologies Corp.’s platform to conduct voting on initiatives and amendments to bylaws, selection of delegates, and election of officers. Also, in September 2017, the Tufts University student union conducted its elections using the Voatz platform, which resulted in higher student voter turnout and lower costs.

In March 2018, two counties in West Virginia began allowing its overseas military, other expatriates eligible under the Uniformed Overseas Citizens Absentee Voting Act (UOCABA), and their dependents and spouses to cast votes in the state’s primary election on Voatz. In November 2018, West Virginia extended the voting platform’s use to its midterm elections. The blockchain voting platform was available to qualified overseas individuals from 24 West Virginia counties. After the midterms, Secretary of State Mac Warner reported that the use of the blockchain voting platform had been extremely successful, with approximately 144 military

---

1998 Id.
1999 Id.
and overseas West Virginians having voted from 30 different countries via the blockchain application.  

15.2 Virtual Currency for Campaign Contributions

The Federal Election Campaign Act (FECA), enacted in 1971 to increase transparency in the political process, is the primary federal statute regulating campaign fundraising and spending. FECA requires that every political committee have a treasurer, who is responsible for authorizing all expenditures, receiving all contributions, recording all contributions, and recording the identities of contributors who make contributions in excess of $50. The Federal Election Commission (FEC), the regulatory agency established to enforce campaign finance laws, requires treasurers to examine all contributions for evidence of illegality and to determine whether such contributions exceed statutory limits.

 FECA establishes provides various contribution limits depending on the status of the contributor and the receiving party. For example, FECA prohibits a person from donating more than $2,000 (as adjusted for inflation) per election to a candidate or a candidate’s political committee, $25,000 (as adjusted for inflation) per year to a national political party committee, or $5,000 per year to a political action committee. Similarly, a multicandidate political committee may not donate more than $5,000 per election to a candidate or a candidate’s political committee, $15,000 per year to a national political party committee, or

---

2010 52 U.S.C. § 30102(a) - (b).
2015 11 C.F.R. § 103.3(b).
2019 See 52 U.S.C. § 30116(a)(4) (a political committee that has been registered for at least 6 months, has at least 50 contributors, and has made contributions to at least 5 federal candidates).
$5,000 per year to a political action committee.\(^{2022}\) The contribution limits apply to money\(^{2023}\) as well as to donations of goods and services.\(^{2024}\) 

In 2014, the FEC concluded that virtual currency falls within the definition of a “contribution” because it is “money or anything of value.”\(^{2025}\) Therefore, contributors may contribute virtual currency to a political committee, which is then obligated to determine the contributor’s identity (e.g., by requiring all contributors to identify themselves) and the legality of the contributions.\(^{2026}\) If the contribution is illegal (e.g., if made by a bank\(^ {2027}\) or federal contractor,\(^ {2028}\) or made in the name of another\(^ {2029}\)) or the amount exceeds contribution limits based on the value of the contributed virtual currency at the time of receipt,\(^ {2030}\) then the political committee must return the illegal or excess amounts.\(^ {2031}\) Although the FEC generally requires contributions to be deposited into a bank account,\(^ {2032}\) a political committee that receives virtual currency may maintain the contribution in a virtual currency wallet, similar to holding non-monetary assets such as securities in a brokerage account.\(^ {2033}\)

The political committee must report the virtual currency contribution when it is initially received, as an in-kind contribution and as a disbursement, thus leaving the cash on hand unchanged while holding virtual currency outside its bank account.\(^ {2034}\) The committee must also report when it liquidates the virtual currency.\(^ {2035}\) If the purchaser is known, the sale is to be reported as a contribution by the purchaser, and the report must include the purchaser’s

\(^{2022}\) 52 U.S.C. § 30116(a)(2)(C); 11 C.F.R. § 110.2(d).


\(^{2026}\) Id.

\(^{2027}\) 52 U.S.C. § 30118(a) (prohibiting contributions by national banks); 11 C.F.R. § 114.2(a).

\(^{2028}\) 52 U.S.C. § 30119(a); 11 C.F.R. § 115.5.

\(^{2029}\) 52 U.S.C. § 30122; 11 C.F.R. § 110.4(b).


\(^{2031}\) 11 C.F.R. § 103.3(b).

\(^{2032}\) 11 C.F.R. § 103.3(a).

\(^{2033}\) Fed. Election Comm’n., supra note 2025.

\(^{2034}\) 11 C.F.R. § 104.13(a); Fed. Election Comm’n., supra note 2025.

\(^{2035}\) Fed. Election Comm’n., supra note 2025.
identification.\textsuperscript{2036} If the purchaser is unknown, the political committee must report the sale with information as to the exchange, date of sale, and value of virtual currency at time of sale.\textsuperscript{2037}

In addition to receiving virtual currency contributions, the FEC permits political committees to purchase virtual currency as investments.\textsuperscript{2038} The committee, however, may not use the virtual currency to pay directly for goods or services, and instead must liquidate it first and deposit the proceeds into its bank account.\textsuperscript{2039} Any earnings or losses from the virtual currency investment must be reported as such.\textsuperscript{2040}

Many states are also establishing guidelines for digital currency campaign contributions. In September 2018, California’s Fair Political Practices Commission voted to ban political donations with any virtual currency.\textsuperscript{2041} Other states such as South Carolina\textsuperscript{2042} and North Carolina\textsuperscript{2043} have also banned virtual currency contributions. States such as Colorado,\textsuperscript{2044}

\textsuperscript{2036} 11 C.F.R. § 104.13(b); Fed. Election Comm’n., supra note 2025.
\textsuperscript{2037} 11 C.F.R. § 104.13(b); Fed. Election Comm’n., supra note 2025.
\textsuperscript{2038} Fed. Election Comm’n., supra note 2025.
\textsuperscript{2039} Id.
\textsuperscript{2040} 52 U.S.C. § 30104(b)(3)(G); 11 C.F.R. § 104.3(a)(3).
\textsuperscript{2042} Advisory Opinion 2018-3, South Carolina House of Legislative Ethics Committee (Apr. 11, 2018), https://www.scstatehouse.gov/CommitteeInfo/HouseEthicsCommittee/AdvisoryOpinions/HEC%202018.3.pdf.
Massachusetts, \textsuperscript{2045} Tennessee, \textsuperscript{2046} and Montana \textsuperscript{2047} permit virtual currency donations with certain restrictions.


\textsuperscript{2046} Tenn. Code Ann. § 2-10-113(a) (emphasis added); see also id. § 2-10-102(4) ("‘Contribution’ means any advance, conveyance, deposit, distribution, transfer of . . . digital currency . . . made for the purpose of influencing [an election]."). Tennessee may be the only state that has enacted legislation regarding the receipt of cryptocurrency by candidates and political committees.

Chapter 16

16 Executable Distributed Code Contracts

16.1 What are EDCCs?

EDCC is the acronym used in the blockchain community for an “executable distributed code contract.” In its simplest form, an EDCC – often erroneously referred to as a “smart contract” – is a self-executing electronic transaction or agreement that operates on a blockchain. In technical terms, an EDCC is a programmable object on a blockchain that is governed through a set of code-instructions that execute transaction(s) between two or more parties. 2048

Since 2015, EDCCs have gained considerable attention for their implementation in the financial industry as a new way to manage shares, bonds, or derivatives contracts. Articulating such transactions into code has allowed financial markets to become more automated and has simplified many process-intensive systems related to the trading and servicing of financial instruments. 2049 As blockchain technology has matured, other assets have also been stored and traded over blockchain networks, such as real estate 2050 and intellectual property. 2051 EDCCs are expected to be usable for any type of exchange of value or information between two or more parties, including transferring title to real or personal property, managing marriage, divorce, and child custody agreements, placing bets in fantasy sports leagues, payments on loans, licensing agreements and nearly every other type of transaction that can be documented in a traditional contract.

16.1.1 The History and Development of EDCCs

The concept of an EDCC was first proposed in the 1990s. Nick Szabo’s paper The Idea of Smart Contracts offered a simple analogy to explain the theory. Consider a transaction where money is deposited into a vending machine in exchange for a drink. 2052 Inserting money triggers a set of actions resulting in the automatic dispensing of a drink. 2053 Once money is inserted into the vending machine, the transaction cannot be paused or stopped midway. 2054 Furthermore, the money can no longer be returned once the drink is supplied. This is essentially how an EDCC works. Once an EDCC is coded on a blockchain ledger, the instant a triggering action occurs (e.g., depositing the money), the contract executes all other actions specified by the parties (e.g.,

2051 https://www.ascribe.io.
2053 Id.
2054 Id.
dispensing a drink). The triggering actions are predetermined by the parties, coded into the EDCC, and stored on the blockchain. Once the transaction is triggered, it cannot be interrupted or reversed.

The Ethereum network was the first to implement EDCCs on a decentralized distributed platform, allowing users to code instructions to self-execute the terms and conditions of an EDCC. As first outlined in the Ethereum whitepaper, the “Ethereum protocol was originally conceived as an upgraded version of a cryptocurrency, providing advanced features such as on-blockchain escrow, withdrawal limits, financial contracts, gambling markets and the like via highly generalized programming language.” Interestingly, however, the protocol does not directly support any of the decentralized applications that were built on the platform; instead, the existence of Ethereum’s Turing-complete programming language allows decentralized applications (DApps), and thus EDCCs, to be created for any transaction, agreement, or application by a user.

The code parameters (i.e., instructions) of an EDCC are defined by its creator, but an EDCC’s automated execution of the instructions are supported by a blockchain’s network. The code is written in a low-level, stack-based bytecode language referred to as “Ethereum virtual machine code” or “EVM code,” which consists of a series of bytes, each representing an operation. EDCCs are then built with cryptographic “boxes” that contain value and only unlock if certain conditions are met, enabling parties to formally establish a cryptographical transaction or enforceable agreement. Depending on the specific code, the execution of one transaction can in turn trigger that of various other transactions through “messages” that the EDCCs can send to one another. As a result, EDCCs can establish relationships with other EDCCs in the virtual world in the same manner as external actors in the physical world.

By developing this technology, Ethereum has effectively discovered a way to integrate law and economics with cryptography. Users can embed different types of contractual clauses into the software and form an enforceable agreement, the breach of which may result in the immediate enforcement of the terms of the EDCC. Additionally, all parties privy to the transaction can see the development of the contract step by step, enhancing trust among the parties during the contracting process.

By way of example, Ann’s grandmother agrees to let Ann purchase her car for $30 on Ann’s 18th birthday. In order to ensure the maximum enforceability of this arrangement, a written agreement is drafted and signed. Thereafter, upon Ann’s 18th birthday, Ann will have to pay her grandmother, coordinate the transfer of title from her grandmother’s name to her own, and update her car insurance to reflect her new car, making it a lengthy process. However, if all of these actions are instead placed on an EDCC with Ann and her grandmother agreeing to the same terms, the actions are automated and executed on the blockchain.

---


2057 Id.

2058 Id.

2059 Id.
immediately upon Ann’s 18th birthday, the EDCC will automatically deduct $30 from Ann’s wallet and place it into her grandmother’s wallet. Then the EDCC code will transfer the car title into Ann’s name, inform both parties that the transfer has occurred, and automatically update Ann’s car insurance with the change.

Using this simple hypothetical, it is easy to see how EDCCs can significantly simplify people’s lives through their self-executing nature. Despite such transparencies, efficiencies, and cost reductions, however, EDCCs have been criticized as too rigid to adapt to the changing circumstances of the real world. This is because once an EDCC goes live, it is unalterable and will operate automatically according to the code set by its creator. While it is possible for parties to build safety controls into the EDCC to halt the execution of the transaction through mutual agreement, it is difficult for parties to foresee all potential circumstances where the halting of an EDCC may be deemed necessary.

16.2 EDCCs Versus “Smart Contracts”

EDCCs are often referred to as “smart contracts,” which can be misleading. The term “smart contract” is most often used in the computer science industry to identify a specific technology – i.e., code that is stored, verified and executed on a Turing-complete blockchain. Despite most blockchain literature referring to EDCCs as “smart contracts,” there is a fundamental disconnect between what these ‘contracts’ are called and what they actually do.

The adjective “smart” implies intellectual skill and suggests a dynamic nature to the underlying tool. “Smart” may also seem to suggest that the code uses artificial intelligence or big data. However, a “smart contract” is notable for its automated features, not for its ability to predict the outside world. Blockchain-based contracts, similar to computers, cannot think for themselves. Instead, EDCCs only perform the tasks they were programmed to perform. This is the case even if an EDCC draws data from an oracle in the non-blockchain world. Regardless

2063 De Silva, supra note 2056.
2064 Id.
2065 Id.
2066 Oracles help connect users to a data source and (sometimes) verify that the result of the user's query is correct.
of whether an oracle is present, the code requires built-in parameters to guide the transaction in its entirety.

Since decentralization and automation are the key features of blockchain-based contracts, the term Executable Distributed Code Contract (EDCC) more accurately reflects the vital nuances of these traits.

16.3 Types of EDCCs

16.3.1 Transactions

A transaction is an exchange of value between two or more parties. However, unless the transaction calls for simultaneous performance, at least one party is always promising to deliver their promised performance at some point in the future, thus creating a constant uncertainty that one of the parties will renege. Using the example of Ann and her grandmother above, if Ann’s grandmother simply promised to gift Ann the car instead of making Ann pay for it, this would be a transaction in which Ann would be uncertain if her grandmother will actually perform.

Additionally, not all transactions include legally enforceable mechanisms in the event that the transaction is not carried to completion. Using the same example, if Ann’s grandmother promised to gift Ann the car and failed to do so, Ann would have no legal recourse for her grandmother’s broken promise. While other enforcement mechanisms may exist, such as risk to reputation or even “self-help,” without a legal enforcement mechanism, a party can only hope for the other’s compliance.

16.3.2 Contracts

A contract, however, is a promise or set of promises, the breach of which the law provides a remedy for, or the performance of which the law in some way recognizes a duty. To have a binding, legally enforceable contract, the following elements must be present:

1) *An Offer* – One party (the offeror) must express a manifestation of intent to contract with certain and definite terms and communicate such to another party (the offeree). It is important to note that the terms must be certain and definite. The more vague and ambiguous the terms are, the less likely a court will find that the parties intended the transaction to be binding.

2) *Acceptance* – Once an offer has been made, the offeree must accept the offeror’s offer before it expires or is revoked. An acceptance requires the offeree to manifest assent to the terms of the offer and communicate such intent to the offeror.

---


2069 Restatement (Second) of Contracts § 1 (1981).

2070 *Id.* at § 24.

2071 *Id.* at § 33.

2072 *Id.* at § 30.
3) **Consideration** – Consideration is a bargained for exchange between parties of legal value.\textsuperscript{2073} Courts have defined “legal value” to mean more than sham consideration.\textsuperscript{2074} Consideration can include a promise to perform or a promise to forebear as long as it benefits the other party. However, a gift, an illusory promise (e.g., the ability to cancel the contract at any time), or nominal consideration are all insufficient to satisfy this element.\textsuperscript{2075}

4) **No Defenses** – Finally, even if a contract is formed, it can be held to be void or voidable if a defense exists. Common defenses include lack of capacity (infancy, incompetency or intoxication), failure to be in writing (which only applies to certain contracts), illegal subject matter, misrepresentation or non-disclosure, duress, ambiguity, and or unconscionability.\textsuperscript{2076}

### 16.4 EDCCs as Enforceable Contracts

Through the creation of an EDCC, two or more parties have the ability to meet all of the traditional elements for contract formation, offer, acceptance, consideration and no defenses, thus forming an enforceable agreement.

In recent years, courts have become more permissive in allowing contracts to be formed through the use of new technologies. For example, EDCCs may evolve like “clickwrap agreements.”\textsuperscript{2077} Courts have held such agreements to be enforceable, recognizing that in the modern world, parties do not need to consider and negotiate every term.\textsuperscript{2078} However, all parties still must have notice of the existence of the terms of the contract.\textsuperscript{2079} Whether notice of a term is sufficient will depend on how conspicuous the term is, whether the parties have had a prior course of dealing with one another, and industry norms.\textsuperscript{2080} Furthermore, the terms must be available to both parties during the contracting process. For example, courts have found that clicking a “yes” button in connection with transmitting credit card data does not bind the purchaser to any terms emailed to the purchaser after the enrollment process was completed.\textsuperscript{2081}

---

\textsuperscript{2073} See Id. at § 71.


\textsuperscript{2076} Bill Marino, *Unpacking the Term ‘Smart Contract*,* Medium (Feb. 10, 2016)* [https://medium.com/@ConsenSys/unpacking-the-term-smart-contract-e63238f7db65](https://medium.com/@ConsenSys/unpacking-the-term-smart-contract-e63238f7db65); Restatement (Second) of Contracts (1981); 1 Williston on Contracts (rev. ed. 1936); Murray on Contracts (1974).

\textsuperscript{2077} A "clickwrap agreement" is one formed over the Internet when a website posts terms and conditions and the user clicks an "I accept" button.

\textsuperscript{2078} See, e.g., *Hill v. Gateway 2000, Inc.* (7th Cir. 1997), 105 F.3d. 1147, 1150.

\textsuperscript{2079} See *Register.com, Inv. v. Verio, Inc.* (2nd Cir. 2004), 356 F.3d 393, 403.

\textsuperscript{2080} See *Schnabel v. Trilegiant Corp.* (2nd Cir. 2012), 697 F. 3d 110, 121-22.

\textsuperscript{2081} Id.
With this in mind, in order to form a legally enforceable EDCC, it will be important for the contracting parties to consider how they will give assent to the terms and conditions of the contract and ensure that the parties have had sufficient notice of the contract terms.

In addition to the above elements, which are required to form any enforceable contract, contracts are governed by two different bodies of law, depending on the subject matter of the contract. Contracts that involve the sale of goods are governed by each state’s adoption of the Uniform Commercial Code, while contracts that do not involve the sale of goods are governed by each state’s common law. The two bodies of law adopt different approaches in determining the terms of the contract, performance of the contract, and what may constitute a breach.

16.4.1 EDCCs and Common Law

Common law is the body of law that is based on decisions made by courts in cases. Generally, it applies to contracts involving real estate, personal services, such as employment, and any other subject matter that does not involve the sale of goods. Under common law, substantial performance of the promise invokes performance by the other party. That is to say, even if the performance is not perfect, the other party must perform if there was substantial performance. Although a breach may still exist if perfect performance is not tendered, a minor breach does not excuse the other party from performing their obligations under the contract. The only instance where a party’s performance is excused is when there has been a material breach by the other party. Under the common law, EDCCs may encounter some difficulty when they include terms that are subjective or when a breach occurs.

Contracts have either operational or non-operational clauses, and thus not all clauses are susceptible to automation and self-execution. For example, employment, consultant and independent contractor agreements often have non-operational clauses such as the use of the terms “best efforts” or “good faith” to describe the obligations required by the party performing the services. First, these terms are subjective, making it nearly impossible for a code to be programmed to recognize when these terms have been met or breached. Additionally, the definitions of these terms vary greatly among jurisdictions. Therefore, parties will either need to have a human element to EDCCs that requires a human to sign off on the meeting of the subjective term, or the parties will need to create a specific, measurable set of requirements, instead relying on subjective variables that need human verification. Even so, it is undoubtedly impossible to predict all possible variations under such contracts.

Furthermore, as discussed above, the common law only allows a party to suspend its performance under the contract if the other party has materially breached. Again, the creator of an EDCC may have difficulty creating code that automatically recognizes when a material breach has occurred. To avoid such uncertainty, parties to an EDCC could create a list of specific situations that would amount to a material breach, thus allowing the code to self-execute and notify the parties when a material breach has occurred and pause the EDCC. However, this option will only be a viable if the material breach is recognizable by its code. Minor breaches are less

---

2082 Goods are defined as movable, tangible things. (U.C.C. Article 2, § 2-105(1)).

problematic since they typically result in the non-breaching party being awarded damages, which they can recover through the judicial system or some other blockchain-based online dispute resolution applications, as discussed below.

16.4.2 EDCCs and the Uniform Commercial Code

All U.S. states have adopted a form of the UCC, which governs all contracts involving the sale of goods. While sections of the UCC delineate between merchants (i.e., a car dealer) and non-merchants (i.e., an average person), if the sale of goods is involved, even a private sale between two parties, then the agreement is governed by the UCC that was adopted by the state where the transaction occurs.

Unlike common law, the UCC requires that parties deliver “perfect tender.” Meaning, they must perform exactly as they promised in the agreement. If one of the parties fails to perform as promised, it constitutes a breach and entitles the non-breaching party to suspend performance. While the UCC varies in several other ways from the common law, such differentiations are not generally relevant to the enforceability of an EDCC.

EDCCs that involve the sale of goods will be easier to form and execute since those agreements are governed by each state’s adoption of the UCC instead of the common law. Typically, contracts for the sale of goods have fewer subjective terms than other types of contracts. Thus, parties will be able to code specific terms such as price, quantity of goods, delivery date, and shipping parameters – all of which are subject to automation and self-execution.

Additionally, as detailed above, the UCC requires performance of the contract to be a perfect tender. An EDCC can be coded to automatically recognize a breach when the goods have or have not been delivered. For example, if a pen manufacturer contracted to send a buyer 100 pens and instead only sends 50, the EDCC would automatically recognize the breach and halt the EDCC before deducting the contract price from the buyer’s wallet. Granted, thereafter, the parties may need to discuss whether the buyer will agree to accept or reject the non-conforming goods, but the vast majority of the terms in the agreement are capable of self-execution by the EDCC.

16.4.3 EDCCs and the Statute of Frauds

Certain contracts must be in writing, which in legal vernacular is referred to as “falling under the Statute of Frauds.” The law requires a writing because some contracts are more susceptible to fraud than others or involve a valuable exchange that must be in writing to ensure that the parties have a meeting of the minds. Contracts that fall under the Statue of Frauds, and thus must be in writing, are:

1) A promise in consideration of marriage (i.e., a promise to do something or refrain from doing something if two people marry);
2) Contracts that are incapable of being performed within one year from the date of the agreement;

---

2084 Merchants are defined as "a person who deals in goods of the kind . . . involved in the transaction." (U.C.C. Article 2, § 2-104(1)).
2085 U.C.C. Article 2, §2-601.
3) Transfers of interest in real estate for more than one year, including all real estate sales;
4) Promise by an executor to answer personally for the debt of the decedent;
5) Sale of goods amounting to $500 or more; and
6) Promise by a surety to answer for the debts of another (i.e., guaranties). 2087

In order to satisfy a writing under the Statute of Frauds, the writing must identify the parties, identify the contract’s subject matter, include the material terms and conditions of the contract, and be signed by the person to be bound. 2088 While there are a few exceptions where the courts permit performance, instead of a writing, to satisfy the statute of frauds, for the purposes of this chapter those exceptions will not be discussed.

For contracts that require a writing under the Statute of Frauds, EDCCs will meet this writing requirement. Under the Federal Electronic Signatures in Global and National Commerce Act of 2000, 2089 written electronic agreements are considered legally binding. Similarly, under the Uniform Electronic Transactions Act, adopted by 47 states, transactions may be conducted by electronic means and the Act gives legal recognition to electronic signatures, records and contracts. Additionally, common law permits extrinsic writings to be incorporated into a legally binding agreement. Therefore, in the event that an agreement is entered into through traditional paper-to-paper format, the agreement may still call for certain terms to be performed on the blockchain, creating a hybrid agreement. Under the common law, specifically incorporating those terms into the writing would be sufficient for enforceability in the event that some of the terms are carried out through an EDCC.

While most state laws would also recognize an EDCC as a writing, some states are passing legislation to eradicate any confusion. In March 2017, Arizona signed a bill to clarify and confirm that “a signature that is secured through blockchain technology is considered to be in electronic form and to be an electronic signature.” 2090

16.5 Challenges to Enforcement of EDCCs

One of the main benefits of a contract is its legal enforceability. Through the years, society has developed certain enforcement mechanisms to instil confidence among parties to a contract. Such enforcement mechanisms are usually handled in a court of law.

2089 “Notwithstanding any statute, regulation, or other rule of law (other than this subchapter and subchapter II of this chapter), with respect to any transaction in or affect interstate or foreign commerce (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.” 96 U.S.C. § 7001(a).
2090 HB 2417.
Certain EDCCs, based on their terms, may not require enforcement due to the automatic nature of the technology. However, enforcement may pose a challenge when EDCCs are executed incorrectly, contain terms that cannot be performed by code, or where parties have decided outside of the EDCC to change the terms.

In the traditional sense, there may be some challenges to initiating legal action to enforce an EDCC. For example, to be subject to a court’s jurisdiction, participants in a blockchain transaction will need to identify themselves and submit to the jurisdiction of the relevant court. Since EDCCs are distributed multi-jurisdictional applications, this can pose significant challenges in determining which courts have personal and subject matter jurisdiction over the parties and the dispute. To avoid such identification issues, the contracting parties will either need to reveal their identities or identify an agent in the EDCC who will be responsible for being named should a lawsuit be filed. Parties to EDCCs whose anonymity is a priority will need to decide whether having legal recourse or remaining anonymous is most important. Additionally, parties that do not reside in the same state and want enforcement of the EDCC to be conducted through a court of law should include a governing law provision in their EDCCs so as to avoid conflicting state laws.

A final barrier is the public’s unfettered access to legal records filed in federal and state courts. The American legal system is premised on allowing the public to view legal proceedings, and legal documents filed in those proceedings are generally a matter of public record. Thus, anyone wanting to access information on a case can request and receive any filed documents. Parties to an EDCC that reveals trade secrets or sensitive information may not want to have their dispute available to the public. While courts do permit parties to request the sealing of documents to protect proprietary information, this is an arduous process and not always granted by the court.

16.5.1 Blockchain-based Enforcement Mechanisms

Arguably the most feasible and cost-effective approach to contract enforcement is through third-party arbitration. Arbitration is much cheaper than litigation and offers a quicker resolution. Traditional arbitration is conducted through a third-party neutral who assists in determining a fair resolution to a dispute.

Undoubtedly, users who enter legally enforceable EDCCs would prefer the enforcement of such EDCCs to occur directly through the EDCC than through a court of law or traditional arbitration. Consequently, many companies are developing DApps that allow parties to agree at the outset of the EDCC to specific procedures for the resolution of disputes. This allows users to maintain their pseudo-anonymity, jurisdictional issues would be moot, proprietary information would remain confidential, and tribunals would be comprised of individuals with specialized technical knowledge, instead of a jury of peers. Many arbitration start-ups are building DApps to resolve disputes arising out of blockchain transactions.


16.5.1.1 Aragon Network

The Aragon Network is another avenue for dispute resolution. At the outset of the EDCC, the parties would need to surrender to Aragon’s jurisdiction. To begin proceedings, a party must post a bond in ANT tokens to be used as collateral. If the party wins, they receive their tokens back; if they lose, the tokens are retained. In extreme situations, the platform even has the ability to freeze all of the defendant’s contracts and business transactions.  

When proceedings begin, five judges are selected at random from Aragon users who have expressed a willingness to settle disputes by filing deposits in tokens. Similar to Dartella, the Aragon Network has created their own jurisdictional rules and reviews the claims, evidence and defenses for the case. Thereafter, each judge makes an individualized decision and sends their encrypted decision to the court. To avoid collusion, each judge is prohibited from revealing his or her decision to the other judges until the deadline for submitting a verdict has passed and the court announces the decision. If a decision is not made, the judges will be fined in ANT tokens. Similarly, judges who made the “correct” decision will be rewarded with “reputation” tokens while those who made a losing decision will be penalized.

If the party is unsatisfied by the panel’s judgment, it can post a larger bond to seek an appeal. The appeal level operates under the rules of a prediction market and permits all Aragon judges to participate in resolving the dispute in the same manner as above. If the party posting the bond is still unsatisfied by the result, it can post bond to the Supreme Court of the Aragon Network, composed of the top nine judges ranked by Aragon Network Jurisdiction pay-out.

16.5.1.2 Kleros

Kleros relies on game theory, cryptography and blockchain systems. Similarly to other DApps, parties to an EDCC agree to use Kleros as their adjudication protocol. The parties create and put money into escrow accounts for security. Once a dispute arises, the relevant information is sent to Kleros through the blockchain. Kleros allows individuals to sign up as jurors for the service and provides incentives to make honest decisions. Kleros panels an anonymous jury from its pool, and the number of jurors depends on the number agreed upon at the outset by

2094 Id.
2096 Jurors voting coherently with the majority are rewarded with money, whereas jurors voting incoherently or who are dishonest lose money.
2098 Id.
the parties. The jurors then evaluate the evidence and cast a vote in favor of one party.\textsuperscript{2099} If a party is not satisfied with the decision, it can appeal the case to a new tribunal. The decision is enforced directly through the EDCC or a Kleros partner. For example, once a jury decides fault, it can pass the information to a social media platform that enforces the decision by taking away reputation points from the breaching party.\textsuperscript{2100}

\textbf{16.5.1.3 Jury.online}

In October 2017, Jury.online, announced that it created a protocol for interaction between jurors or arbitrators and the parties to a deal, claiming that the platform is transparent, secure and convenient for making deals using blockchain and other cryptographic systems.\textsuperscript{2101} Built on the Ethereum blockchain, Jury.online explains that to use the service, the parties’ EDCC must include a provision for dispute resolution through Jury.online. The parties to the EDCC then deposit funds for the service. Jurors from around the world, who specialize in an industry, can join and specify the price for which they are willing to work. If a dispute arises, users are connected with randomly selected jurors who make legal decisions and render a judgment regarding the dispute. Jurors are then paid via the Jury.online currency, the JOT. If no dispute arises, the funds are returned to each party.\textsuperscript{2102}

\begin{flushleft}
\textsuperscript{2099} Id.
\textsuperscript{2100} Id.
\textsuperscript{2101} Iyke Aru, \textit{A Decentralized Dispute Resolution Platform Emergence on the Blockchain}, Coin Telegraph (Oct. 23, 2017), \url{https://cointelegraph.com/news/a-decentralized-dispute-resolution-platform-emerges-on-the-blockchain}.
\end{flushleft}
Chapter 17

17 Litigation Issues

Blockchain technology has the potential to completely reinvent the way people interact as consumers and in society at large. By providing a system for individuals to transfer data and cryptocurrency with one another directly, safely, securely, and immutably using electronic distributed code contracts, this promising technology can conceivably eliminate the middleman from many transactions. It has been used to create new organizations and has the capability to host a multitude of data platforms, from intellectual property records to the content of social media networks. At the same time, inherent aspects of blockchain technology, including its anonymity and decentralization, present complications for existing litigation frameworks.

17.1 Holding Parties Accountable

17.1.1 Identification of Individuals

Generally, when initiating litigation, a plaintiff knows the identity of, and will name, the defendant in the complaint. In some situations, though, the identity of the defendant is unknown. The decentralized and anonymous nature of blockchain technology poses difficulties when attempting to identify a person or company to hold accountable for misconduct occurring on a blockchain. For example, while anyone can view all of the non-encrypted transactions on a public blockchain, information concerning the identities of participants in those transactions is not available. Certain virtual currency exchanges and decentralized applications (DApps have customer records pursuant to anti-money laundering (AML) and “know your customer (KYC) rules because they are engaged in activities requiring money service business registration with FinCEN2103 and money transmitter licenses under state laws.2104 But many other organizations in the crypto community do not keep such customer and user information on file, making it impossible to identify the counter-party in a transaction.

When a defendant’s identity is unknown, courts typically permit plaintiffs to name an unidentified person as a Doe defendant in the complaint, and, after identification of the party through discovery, amend the pleadings to reflect the party’s true name.2105 However, this type of Doe filing is only useful if the plaintiff is ultimately able to ascertain the defendant’s identity.

To the extent that there is a third-party that potentially has information concerning the identity of a Doe defendant, a plaintiff in federal court may seek the identity of unknown individuals through a discovery subpoena pursuant to Federal Rule of Civil Procedure 45. Discovery subpoenas have been successfully served on virtual currency exchange sites in the past

2103 See Chapter 6, Section 6.3.1 (Federal AML Framework).
2104 See Chapter 4, Section 4.2.2 (State Laws for the Licensing of Money Transmitters and Money Services Businesses).
2105 Federal courts may permit fictitiously named defendants in federal question cases if there is a justification for why the defendant is unknown. See Maclin v. Paulson, 627 F.2d 83, 87 (7th Cir. 1980); Dean v. Barber, 951 F.2d 1210, 1214-16 (11th Cir. 1992). However, this is not always true in diversity cases, where complete diversity is required, Fifty Assocs. v. Prudential Ins. Co. of Am., 446 F.2d 1187, 1191 (9th Cir. 1970); see also Cal. Civ. Proc. Code § 474.
for relevant customer information, as in the Cryptsy litigation where a court-appointed receiver served subpoenas on Coinbase and Bittrex, LLC for the account records of certain customers.\textsuperscript{2106} However, the subpoena process will not be productive for entities that are not legally obligated to maintain customer records, such as a Decentralized Autonomous Organization (DAO). Indeed, the very nature of such organizations means they may have no offices or registered agents for service of process, making it impossible to serve them with a subpoena.\textsuperscript{2107}

If subpoenaed for such information, a third-party may file objections,\textsuperscript{2108} move to quash or modify the subpoena,\textsuperscript{2109} or move for a protective order.\textsuperscript{2110} If objected to, the serving party must file a motion to compel the third-party’s compliance in the court where compliance is required.\textsuperscript{2111} District courts and particular judges may also have detailed procedures for parties to follow in order to file discovery motions, such as pre-motion conferences and preparation of joint documents.

Serving a subpoena and ensuring compliance can be challenging and costly. Whether such efforts are worth the time and expense depends on the value of a case and the likelihood of identifying a defendant who can ultimately satisfy a judgment.

\textbf{17.1.1.1 Identification of Parties in Copyright Infringement Cases}

Individuals or companies tasked with identifying infringing parties in matters involving blockchain technology – e.g., selling copyrighted material or storing copyrighted material in an IP registry on a blockchain – should consider the Online Copyright Infringement Liability Limitation Act (OCILLA), which was enacted in 1998 as part of the Digital Millennium Copyright Act.\textsuperscript{2112} The OCILLA gives copyright holders the power to subpoena a service provider\textsuperscript{2113} for the identity

\begin{thebibliography}{99}
  \bibitem{2107} What is DAO, CoinTelegraph, \url{https://cointelegraph.com/ethereum-for-beginners/what-is-dao} (last visited Nov. 21, 2018).
  \bibitem{2109} Rule 45 requires a court to quash or modify a subpoena that “(i) fails to allow a reasonable time to comply; (ii) requires a person to comply beyond the geographical limits specified in Rule 45(c); (iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or (iv) subjects a person to undue burden.” Fed. R. Civ. P. 45(d)(3)(A).
  \bibitem{2110} See Fed. R. Civ. P. 26(b)(2)(C) (describing circumstances where a protective order is appropriate).
  \bibitem{2112} 17 U.S.C. § 512.
  \bibitem{2113} 17 U.S.C. § 512(k) (“[T]he term ‘service provider’ means a provider of online services or network access, or the operator of facilities therefor,” and includes “an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.”).
\end{thebibliography}
of an individual believed to be downloading unauthorized files containing copyrighted works. Service providers are then obliged to “expeditiously disclose to the copyright owner … the information required by the subpoena.”

In Voltage Pictures, LLC v. Does 1-5,000, 119 potential defendants received letters from their ISPs indicating that they could be sued for downloading unauthorized copies of the movie “The Hurt Locker.” Voltage Pictures alleged the defendants had downloaded the movie via the P2P sharing program BitTorrent. Using a software tracing program, Voltage Pictures discovered the date and time of each unauthorized download of the movie then subpoenaed the relevant IP addresses from various ISPs.

The alleged infringers moved to quash the subpoenas, arguing that they did not engage in the alleged infringement, the subpoenas invaded their First Amendment and privacy rights, and the subpoenas subjected them to undue hardship by requiring them to litigate in a forum that lacked personal jurisdiction over them. The court rejected these arguments, holding that a general denial of liability was not a basis for quashing the subpoenas, the infringers’ asserted rights did not shield them against allegations of copyright infringement, and the infringers faced no undue burden because they were neither parties to the litigation nor under any obligation to produce information in response to the subpoenas.

In Sony Music Entertainment Inc. v. Does 1-40, seventeen record companies sued forty unidentified “Doe” defendants for copyright infringement. The record companies served a subpoena on non-party ISP Cablevision seeking to obtain the defendants’ identities. Four of the defendants moved to quash the subpoena on grounds that the ISP subpoenas violated the First

---

2114 17 U.S.C. § 512(h).
2117 Id.
2119 Id.
2120 Voltage Pictures, 818 F. Supp. 2d at 34-37.
2121 Id.; see also Arista Records, LLC v. Doe 3, 604 F.3d 110 (2d Cir. 2010) (holding that the defendant’s First Amendment rights to anonymity did not warrant the quashing of the recording companies’ subpoena); Dendrite Int’l, Inc. v. Doe No.3, 342 N.J.Super.134, 141 (App. Div. 2001) (In considering whether to compel ISPs to identify anonymous defendant posters, courts must strike “a balance between the well-established First Amendment right to speak anonymously, and the right of the plaintiff to protect its proprietary interests and reputation through the assertion of recognizable claims based on the actionable conduct of the anonymous, fictitiously-named defendants.”).
2123 Id. at 559.
Amendment.\textsuperscript{2123} The defendants argued that people who use the Internet to download copyrighted music without permission are engaged in the exercise of free speech, meaning their identities are protected from disclosure by the First Amendment.\textsuperscript{2124}

The court held the defendants’ use of P2P file sharing and copying qualified as free speech,\textsuperscript{2125} citing \textit{In re Verizon Internet Servs., Inc.}\textsuperscript{2126} Nonetheless, the court concluded that the First Amendment did not bar disclosure of the Doe defendants’ identities\textsuperscript{2127} after considering the following factors: (1) a concrete showing of a \textit{prima facie} claim of actionable harm; (2) the specificity of the discovery request; (3) the absence of alternative means to obtain the subpoenaed information; (4) a central need for the subpoenaed information to advance the claim; and; (5) the party’s expectation of privacy.\textsuperscript{2128}

Application of OCILLA’s subpoena procedure would depend upon whether the third-party fell within the definition of a “service provider.” Even assuming that it did, several key features of blockchain technology could pose hurdles for plaintiffs, most notably that no single centralized organization runs the Ethereum blockchain. While the Ethereum Foundation created the network, it does not maintain a record of users and technically surrendered control to them upon launch. Similarly, DApps built on the Ethereum blockchain may or may not have information concerning their users’ identities.\textsuperscript{2129}

\textbf{17.1.2 Liability Issues for Blockchain Technology Entities}

Just as blockchain technology poses difficulties for identifying the parties liable for misconduct, suing blockchain companies may also present special challenges to the extent that there are no centralized entities to hold liable, whether directly or vicariously. Moreover, even assuming that a plaintiff can identify an entity to sue, the prospective defendant may, under certain circumstances, raise defenses similar to those relied upon by computer hardware manufacturers and providers of interactive computer services like social networks.

\textbf{17.1.2.1 Hardware Manufacturers Liability}

Manufacturers of blockchain technology hardware facing contributory copyright infringement claims may argue they are not liable for selling equipment capable of commercially significant non-infringing uses. While blockchain technology is primarily decentralized and

\textsuperscript{2123} Id. at 559-561.
\textsuperscript{2124} Id. at 562.
\textsuperscript{2125} Id.
\textsuperscript{2127} Sony Music Entm’t Inc., 326 F. Supp. 2d at 564-67.
\textsuperscript{2128} Id.
\textsuperscript{2129} For example, a DApp that keeps track of sports scores probably would not be required to store user information as it likely would fall outside the scope of AML and KYC laws and regulations. By contrast, a payment facilitation DApp might well be required to keep such user records to comply with these laws and regulations.
generally concerned with innovation of software, companies do manufacturer blockchain hardware: in February 2017, Accenture launched a blockchain security hardware, and, in August 2017, Microsoft and Intel launched the Coco Framework, which runs blockchain on hardware using Microsoft Azure.

Hypothetically, if someone involved in the sale of copyrighted material used such security technology to conceal his or her identity, then the hardware manufacturers could be sued for contributory infringement. Also, devices such as physical cold storage wallets have been on the market for some time, and, if a wrongdoer used one to store substantial illicit wealth, the device manufacturer could conceivably be sued vicariously for selling a potentially dangerous product. Although manufacturers of blockchain hardware may be the targets of lawsuits for misconduct by individuals who misuse their hardware, such manufacturers may avoid liability under the precedent set in Sony Corp. of Am. v. Universal City Studios.

In Sony, Universal City Studios commenced a copyright infringement action against Sony alleging that customers had used Sony’s Betamax videotape recorders to illegally record television shows owned by Universal. Universal maintained that Sony was liable for the copyright infringement committed by Betamax users due to how it marketed the Betamax recorder. Universal did not sue any Betamax users, instead seeking damages, an injunction against further manufacturing of Betamax, and equitable accounting of profits all against Sony as the manufacturer of the hardware.

After trial, the District Court sided with Sony, finding that the Betamax users’ copying of material broadcasted over the public airwaves was fair use, that Sony had no direct involvement in the users’ copying, that Sony merely sold a product capable of various uses, including allegedly infringing use, and that an injunction was not warranted as the Betamax hardware could still be used for lawful purposes, such as recording non-copyrighted material or material whose owners consented to the copying. The Ninth Circuit overturned this ruling, holding that Sony was chargeable with knowledge of its consumers’ infringing activity because the copying of

---

2134 Id. at 446.
2135 Id. at 417.
2136 Id.
2137 Id. at 425-27.
copyrighted materials was either “the most conspicuous use” or “the major use” of the Betamax product.\textsuperscript{2138}

Thereafter, the Supreme Court reversed the Ninth Circuit, finding that Sony was not liable for contributory infringement. The Court rejected the theory that Sony was liable for selling its equipment with constructive knowledge that it would be used for infringing purposes.\textsuperscript{2139} The Court also concluded that Sony could not be held contributorily liable because, far from providing Betamax users with Universal’s copyrighted work, Sony merely provided users with hardware “capable of commercially significant non-infringing uses,”\textsuperscript{2140} such as private, non-commercial time-shifting,\textsuperscript{2141} that other copyright holders might welcome.\textsuperscript{2142} The Court further concluded that using Betamax hardware for time-shifting in private homes was fair use because it was a non-commercial, non-profit activity, and because Universal failed to establish any “meaningful likelihood of future harm.”\textsuperscript{2143}

The 1984 decision created a safe haven for home recording devices, and there have been no challenges or significant attempts to overturn the ruling since. Manufacturers of blockchain technology hardware that are sued for providing equipment misused by consumers should consider relying upon the Sony ruling as a defense. Even if blockchain technology hardware is used for illicit purposes, the multitude of other important uses could shield the manufacturers from liability for contributory infringement.

17.1.2.2 Liability of Decentralized Autonomous Organizations\textsuperscript{2144}

Decentralized Autonomous Organizations (DAOs) are virtual entities comprised of a set number of individuals, or “members,” who control the organization’s actions through voting rights.\textsuperscript{2145} Unlike traditional entities, DAOs exist entirely on a blockchain, and their operations are governed by executable distributed code contracts (EDCCs).\textsuperscript{2146} DAOs are currently not recognized as legal entities, thus creating uncertainty over issues such as regulation and liability. Determining legal responsibility for misconduct in a DAO is difficult as DAO membership can be fluid and change in several ways, such as by membership vote or the automatic revocation of an

\begin{footnotes}
\item[2138] \textit{Id.} at 428.
\item[2139] \textit{Id.} at 439.
\item[2140] \textit{Id.} at 442.
\item[2141] “Time shifting” is the practice of recording television for personal use to watch later at a more convenient time.
\item[2142] \textit{Sony Corp. of Am.}, 464 U.S. at 443-46.
\item[2143] \textit{Id.} at 447-56; \textit{see also} Chapter 13, Section 13.1.3 (Copyright).
\item[2144] \textit{See} Chapter 2, Section 2.10 (Decentralized Autonomous Organizations).
\item[2145] CoinTelegraph, \textit{supra} note 2107.
\item[2146] \textit{Id.}
\end{footnotes}
EDCC upon occurrence of certain events. A DAO is essentially a new type of organization, sharing characteristics with informal online groups and formalized corporate entities.

The development of DAOs raises questions regarding how a court could determine who is responsible for misconduct, such as abuse of power, misappropriation of DAO funds, or even money laundering. In the absence of another deep-pocketed party more readily identifiable with the harm, litigants likely would claim that the creators of the DAO (if known) should be jointly liable for any damages caused by a DAO member. If and when corporations law is ever applied to DAO organizations, a DAO could be financially liable for the activities of its creators. Any compensation that the DAO paid could be controlled and enforced through the organization’s EDCCs. If the compensation required was significant, payment could lead to the divesting of funds that the DAO needed to remain operational, damaging the entire DAO by essentially placing liability on the organization as a whole.

It is possible that the creators of a DAO may be unidentifiable. The DAO may have been created by hundreds of anonymous individuals or even by other DAOs, making it difficult, if not impossible, to discover the identities of the creators and hold them liable. Alternatively, one could argue that all members of a DAO should be vicariously liable for any one member’s actions, especially if the members exercise voting rights control and receive direct or indirect financial benefit from the DAO’s operations. If a DAO is deemed similar to a general partnership structure, individual members could be liable in this way. At the same time, there is a certain injustice in holding one member liable for another’s actions when the individuals have never interacted or known of one another, especially if the DAO’s membership is large.

If a DAO is analogous to a corporation or a limited liability company (LLC), the DAO itself (i.e., as an entity) could be held liable for wrongdoing. In that case, individual DAO members would, like shareholders or members in a corporation or LLC, only be liable if the corporate veil was pierced. Since DAOs are not yet considered legal entities, however, there are no legal formalities for them to observe. Until DAOs are required to create corporate organizational structures, courts are unlikely to treat them as legal entities. Compliance with corporate or LLC

---

2147 Id.
2149 Alter ego doctrine (i.e., piercing the corporate veil) allows claimants to hold shareholders liable for the debts of the corporation. Such liability generally requires (1) the shareholders treated the corporation as an alter ego, and (2) allowing the shareholder to escape liability would promote injustice or sanction a fraud. Badian v. Elliott, 165 F. App'x 886, 889 (2d Cir. 2006); Hambleton Bros. Lumber Co. v. Balkin Enterprises, Inc., 397 F.3d 1217, 1227 (9th Cir. 2005); Trustees of Nat. Elevator Indus. Pension, Health Benefit & Educ. Funds v. Lutyk, 332 F.3d 188, 194 (3d Cir. 2003); Stoebner v. Lingenfelter, 115 F.3d 576, 579 (8th Cir. 1997); Sea-Land Servs., Inc. v. Pepper Source, 993 F.2d 1309, 1311 (7th Cir. 1993).
formalities might reasonably require the coding of remedy EDCCs that could provide specific instructions for enforcement of either contracts or remedial injunctions, or for recoveries.2150

In July 2017, the SEC issued a report concluding that the initial offering of tokens by a virtual organization called “The DAO”2151 constituted a sale of securities and should thus have been subject to federal securities law.2152 Consequently, the DAO should have registered with the SEC as per the registration process under section 6 of the Securities Act of 1933.2153 While this provides some clarity as to the legal position of a DAO and what its tokens can represent, absent any organizational structure within a DAO, it remains unclear whose duty it would be to file and register with the SEC or how these requirements could by enforced.

The lack of clarity in the classification of DAOs has led some entities to get creative in protecting themselves from potential liability. For example, in February 2018, the Dash platform, a cryptocurrency project whose website lists its U.S. headquarters as Scottsdale, Arizona, announced that it was the first entity to be legally owned by a DAO.2154 The Dash DAO, as it is named, claims that it is an organized, self-funding entity that has no central authority and is open for any individual to participate.2155 The Dash DAO is owned by The Dash DAO Irrevocable Trust, which was formed in New Zealand. Moreover, Dash masternodes control the company and are the beneficiaries of the trust.2156 The CEO, Ryan Taylor, stated that this legal structure allows Dash Core Group to grow while preventing risks of being shut down in the future.2157 It establishes a fiduciary duty back to the network, he claims, ensuring that Dash Core Group is legally required to act in the network’s best interests.2158

17.1.3 Jurisdiction

17.1.3.1 Subject Matter Jurisdiction

State courts are courts of general jurisdiction, meaning they can hear any case concerning state law and some matters involving federal law.2159 By contrast, federal courts have limited

2150 Wright & De Fillipi, supra note 2148, at 55.
2151 See Chapter 8, Section 8.3.2. (SEC Report on The DAO).
2155 Id.
2156 Id.
2157 Id.
2158 Id.
jurisdiction.\textsuperscript{2160} To hear cases and enforce judgments, federal courts must have both subject matter and personal jurisdiction. Subject matter jurisdiction is defined and limited by the U.S. Constitution.\textsuperscript{2161} In civil matters, subject matter jurisdiction is divided into two types: federal question jurisdiction, where the plaintiff alleges a violation of a federal law, the U.S. Constitution, or a treaty of the United States;\textsuperscript{2162} and diversity jurisdiction, where the parties are citizens of different states and the amount in controversy exceeds $75,000.\textsuperscript{2163}

For diversity jurisdiction, albeit with a few exceptions, federal courts require complete diversity, meaning all the parties on one side of the litigation must be citizens of a state or country different from all parties on the other side.\textsuperscript{2164} The citizenship for a natural person is the person’s state of domicile,\textsuperscript{2165} which is where the person is physically located and intends to remain.\textsuperscript{2166} In making this determination, courts consider various factors, including a person’s voting registration, driver’s license, residency, location of friends and family, business, payment of income tax, location of financial accounts, and intent to remain in the state.\textsuperscript{2167}

A corporation (including a non-profit or professional corporation) is a citizen of both the state or foreign country where it is incorporated and the place where its principal place of business is located.\textsuperscript{2168} To determine the principal place of business, courts use the “nerve center” test, which focuses on “the actual center of direction, control, and coordination, \textit{i.e.}, the ‘nerve center,’” as opposed to “simply an office where the corporation holds its board meetings (for example, attended by directors and officers who have traveled there for the occasion).”\textsuperscript{2169} Limited liability companies and unincorporated entities, such as partnerships and associations, are citizens of the states where each of their members and partners reside.\textsuperscript{2170}

The Class Action Fairness Act of 2005\textsuperscript{2171} (CAFA) provides exceptions to the regular diversity jurisdiction rules for class actions. CAFA permits federal courts to exercise diversity jurisdiction.

\begin{itemize}
\item \textsuperscript{2160} \textit{Kokkonen v. Guardian Life Ins. Co. of America}, 511 U.S. 375, 377 (1994).
\item \textsuperscript{2161} U.S. Const. art. III, § 2 (describing subject matter and diversity jurisdiction).
\item \textsuperscript{2162} 28 U.S.C. § 1331.
\item \textsuperscript{2163} 28 U.S.C. § 1332.
\item \textsuperscript{2164} \textit{Caterpillar Inc. v. Lewis}, 519 U.S. 61, 68 (1996).
\item \textsuperscript{2165} \textit{Galva Foundry Co. v. Heiden}, 924 F.2d 729, 730 (7th Cir. 1991); \textit{Kantor v. Wellesley Galleries, Ltd.}, 704 F.2d 1088, 1090 (9th Cir. 1983).
\item \textsuperscript{2166} \textit{Veranda Assocs., L.P. v. Hooper}, 496 F. App'x 455, 457 (5th Cir. 2012); \textit{Dakuras v. Edwards}, 312 F.3d 256, 258 (7th Cir. 2002); \textit{Lew v. Moss}, 797 F.2d 747, 750 (9th Cir. 1986).
\item \textsuperscript{2167} \textit{O'Connell v. New Jersey Tpk. Auth.}, 649 F. App'x 280, 283 (3d Cir. 2016).
\item \textsuperscript{2168} 28 U.S.C. § 1332(c)(1).
\item \textsuperscript{2169} \textit{Hertz Corp. v. Friend}, 559 U.S. 77, 93 (2010).
\item \textsuperscript{2170} \textit{Carden v. Arkoma Assocs.}, 494 U.S. 185, 195 (1990).
\item \textsuperscript{2171} 28 U.S.C. § 1332(d).
\end{itemize}
jurisdiction over a class action that has at least 100 members in the proposed class if there is minimal diversity and the matter in controversy exceeds $5 million, exclusive of interest and costs.\textsuperscript{2172} Minimal diversity requires that at least one class member (either named or unnamed) is a citizen from a state or country different from that of the defendant.\textsuperscript{2173} Even under CAFA, however, a federal court can – and sometimes must – decline to exercise jurisdiction depending on the circumstances.\textsuperscript{2174}

In the decentralized world, plaintiffs relying on diversity jurisdiction may encounter difficulties establishing citizenship with respect to blockchain technology companies. Since DAOs are not legally recognized as corporations, for example, a DAO would be considered a citizen of the state of each of its members under the regular diversity rules\textsuperscript{2175} and, under CAFA, a citizen of the state where its principal place of business is located and the state under whose laws it is organized.\textsuperscript{2176} However, there is no current legal requirement for DAOs to identify their partners or members, and DAOs have neither traditional places of business nor states of incorporation. Therefore, at this juncture, it appears impossible for a party with a claim against a DAO to obtain subject matter jurisdiction in federal court.

17.1.3.2 Personal Jurisdiction

To render a valid judgment, a federal court must, in addition to subject-matter jurisdiction, also have personal jurisdiction over the defendant.\textsuperscript{2177} To establish personal jurisdiction, (1) the defendant must be properly served, (2) there must be a statutory basis for personal jurisdiction, and (3) exercise of personal jurisdiction must satisfy due process.\textsuperscript{2178} Under the first element, a plaintiff must properly serve the defendant and file the proof of service with the court or else file a waiver of service.\textsuperscript{2179} Under the second element, there must be either a federal statute providing for nationwide service of process or a state statute permitting the court’s exercise of personal jurisdiction.\textsuperscript{2180}

\begin{itemize}
  \item \textsuperscript{2172} 28 U.S.C. § 1332(d)(2), (5).
  \item \textsuperscript{2173} See 28 U.S.C. § 1332(d)(2) (delineating CAFA’s diversity requirement).
  \item \textsuperscript{2174} See 28 U.S.C. § 1332(d)(3) (describing the so-called “home state” exception to CAFA); 28 U.S.C. § 1332(d)(4) (describing the so-called “local controversies” exception to CAFA); 28 U.S.C. § 1332(d)(9) (excluding certain corporate cases, such as securities fraud claims, from CAFA).
  \item \textsuperscript{2175} Carden v. Arkoma Assocs., 494 U.S. 185, 195 (1990); Hummel v. Townsend, 883 F.2d 367, 369 (5th Cir. 1989); Jett v. Phillips & Assocs., 439 F.2d 987, 990 (10th Cir. 1971).
  \item \textsuperscript{2176} 28 U.S.C. § 1332(d)(10).
  \item \textsuperscript{2177} In re Texlon Corp., 596 F.2d 1092, 1099 (2d Cir. 1979).
  \item \textsuperscript{2178} Waldman v. Palestine Liberation Org., 835 F.3d 317, 327 (2d Cir. 2016).
  \item \textsuperscript{2179} Fed. R. Civ. P. 4(k).
  \item \textsuperscript{2180} Trustees of the Plumbers & Pipefitters Nat. Pension Fund v. Plumbing Servs., Inc., 791 F.3d 436, 443 (4th Cir. 2015); Joseph Saveri Law Firm, Inc. v. Criden, No. 15-15534, 2017 WL
Even if the first two elements are met, due process requires that the defendant have sufficient minimum contacts with the forum state such that exercise of personal jurisdiction “does not offend traditional notions of fair play and substantial justice.”\textsuperscript{2181} There are two types of personal jurisdiction consistent with this principle – general and specific. General jurisdiction “requires that the defendant have ‘continuous and systematic’ contacts with the forum state and confers personal jurisdiction even when the cause of action has no relationship with those contacts.”\textsuperscript{2182} “For an individual, the paradigm forum for the exercise of general jurisdiction is the individual’s domicile; for a corporation, it is an equivalent place, one in which the corporation is fairly regarded as at home.”\textsuperscript{2183} For specific jurisdiction,

1) The non-resident defendant must purposefully direct activities or consummate some transaction with the forum or resident thereof; or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws;

2) the claim must be one which arises out of or relates to the defendant's forum-related activities; and

3) the exercise of jurisdiction must comport with fair play and substantial justice, i.e., it must be reasonable.\textsuperscript{2184}

In \textit{Zippo Manufacturing v. Zippo.com},\textsuperscript{2185} a landmark personal jurisdiction case concerning Internet activity, a Pennsylvania federal court exercised specific personal jurisdiction over a defendant website operator based in California.\textsuperscript{2186} In discussing personal jurisdiction, the court stated:

[T]he likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the internet. … Traditionally, when an entity intentionally reaches beyond its boundaries to conduct business with foreign residents, the exercise of specific jurisdiction is proper. Different results should not be reached simply because business is conducted over the internet.\textsuperscript{2187}

The court concluded that exercise of specific jurisdiction was proper. More specifically, the court found the defendant had purposefully availed itself of doing business in Pennsylvania by

\textsuperscript{2182} \textit{Silent Drive, Inc. v. Strong Indus., Inc.}, 326 F.3d 1194, 1200 (Fed. Cir. 2003).
\textsuperscript{2184} \textit{Schwarzenegger v. Fred Martin Motor Co.}, 374 F.3d 797, 802 (9th Cir. 2004)
\textsuperscript{2186} \textit{Id.} at 1119.
\textsuperscript{2187} \textit{Zippo Manufacturing Co.}, 952 F.Supp. at 1124.
conducting electronic commerce with 3,000 Pennsylvania residents and seven Pennsylvania Internet access providers.\textsuperscript{2188} The court further ruled that the plaintiff’s trademark infringement claim arose out of the defendant’s Pennsylvania activities because the plaintiff was a Pennsylvania manufacturer and its injuries would likely occur in the state.\textsuperscript{2189} Finally, the court found that the exercise of personal jurisdiction was reasonable given the state’s strong interest in adjudicating disputes concerning trademarks owned by its residents, the plaintiff’s choice of forum, and the fact that the defendant’s commercial activities in the state outweighed the defendant’s burden in litigating in Pennsylvania.\textsuperscript{2190}

In \textit{Bragg v. Linden Research, Inc.}, an online gaming player sued a California online gaming company and its executive for expropriating his virtual property by nullifying his transactions and freezing his account. The court determined that the California defendants had sufficient minimum contacts with the forum state (i.e., Pennsylvania) to exercise jurisdiction.\textsuperscript{2191} In making this determination, the court cited allegations that the nationwide misrepresentations at issue induced people in Pennsylvania, like the plaintiff, to visit the defendant’s website, enter the game, interact with avatars, and purchase virtual property.\textsuperscript{2192}

In view of the foregoing, for blockchain activity conducted over the Internet, non-U.S. based individuals and entities who participate in alleged wrongdoing may find themselves defending cases in U.S. courts if the plaintiff’s claims are related to activity in the United States. In \textit{Greene v. Mizuho Bank, Ltd.},\textsuperscript{2193} for example, the court exercised personal jurisdiction over a Japanese bank\textsuperscript{2194} for its role in the collapse of the Mt. Gox exchange. The court determined that, under relevant state laws (i.e., Illinois and California), long-arm statutes allowed the exercise of personal jurisdiction to the extent permitted by the Constitution.\textsuperscript{2195}

The court further determined that exercising jurisdiction in California was appropriate since Mizuho Bank’s contacts with that state were sufficient to justify personal jurisdiction and

\textsuperscript{2188} \textit{Id.} at 1126.
\textsuperscript{2189} \textit{Id.}
\textsuperscript{2190} \textit{Id.} at 1125-27.
\textsuperscript{2192} \textit{Id.}
\textsuperscript{2194} The now-defunct Mt. Gox exchange had a bank account with Mizuho. Plaintiffs allege that during the time that Mt. Gox was experiencing trouble, Mizuho halted all withdrawals from the account but allowed deposits to continue. \textit{Greene v. Mizuho Bank, Ltd}, 169 F. Supp. 3d 855, 857-60 (N.D. Ill. 2016).
\textsuperscript{2195} \textit{Greene}, 169 F. Supp. 3d at 860-61.
satisfy due process, and because California had a strong interest in adjudicating the case. However, the court ruled that Mizuho’s contacts with Illinois were insufficient to establish personal jurisdiction there since Mizuho had no transactional contact with the Illinois plaintiff, who, unlike the California plaintiff, only conducted transactions through Mt. Gox.

17.1.4 Dispute Resolution

17.1.4.1 Online Dispute Resolution

With the advent of the Internet, courts have been forced to adapt to the rapidly shifting landscape of disputes. No longer do people and entities interact in just the real world; now they interact virtually as well. The rise of the Internet and e-commerce has increased disputes between people and entities across state and national borders, placing increased pressure on traditional dispute resolution (i.e., the court system) and alternative dispute resolution (e.g., arbitration and mediation) to resolve disputes fairly and efficiently.

One proposal that may prove amenable to online users and parties engaged in Internet transactions is resolving disputes through online dispute resolution (ODR). Although there is no single definition of ODR, the basic idea is to centralize dispute resolution, creating one body to communicate with customers in several languages, and to make requests and directions instantaneous through email or an online platform. An ODR decision could be enforced either in

2196 Id. at 861-62, 863 (Mizuho “accept[ed] [the California plaintiff’s] deposit, knowing that it arrived from a California branch and a California resident, and profiting from the associated fees;” and Mizuho’s failure to disclose that it had stopped cash withdrawals “lulled [plaintiff] into a false sense of security.”).

2197 Id. at 863 (noting that California’s strong interest in providing a forum for its residents seeking redress outweighed any burden faced by a Japanese bank that should have reasonably expected to be hauled into a court in a Mt. Gox user’s home jurisdiction).

2198 The court permitted the plaintiffs to amend their complaint to add an Illinois plaintiff who sent deposits to Mizuho, in order to satisfy minimum contacts requirements for the court to exercise personal jurisdiction. Greene v. Mizuho Bank, Ltd, 169 F. Supp. 3d 855, 865-67 (N.D. Ill. 2016).


2201 “ODR encompasses a broad range of approaches and forms (including but not limited to ombudsmen, complaints boards, negotiation, conciliation, mediation, facilitated settlement, arbitration and others), and the potential for hybrid processes comprising both online and offline elements.” UNCITRAL, Technical Notes on Online Dispute Resolution 1 (Apr. 2017), http://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf.
the courts, like an arbitration ruling, or outside of the judicial system, via user reviews, chargebacks, escrow services, etc.

Currently, there is no globally accepted framework for regulation of cross-border ODR. However, some international organizations have developed platforms for Internet dispute resolution. In 2016, the European Union launched a union-wide ODR platform with translation capabilities, which was created pursuant to Regulation No. 524/2013 and ADR Directive (2013/11/EU). In December 2016, the General Assembly of the United Nations passed a resolution recommending that all states refer to the United Nations Commission on International Trade Law’s Technical Notes on Online Dispute Resolution, a non-binding document that describes and reflects elements of an ODR procedure, including a description of the stages of an ODR proceeding and the scope of the ODR process to apply to transactions for goods or services.

Additionally, private companies have released frameworks for ODR. In January 2018, Kleros published a short paper announcing its development of a “decision protocol for a multipurpose court system able to solve every kind of dispute.” Built on the Ethereum blockchain, the paper explains that “every step of arbitration is automated and the platform does not rely on the honesty of individuals, but on game-theoretical economic incentives.” To use

---


2203 See Marc Grainer *et al.*, *A Promise Unfulfilled and What to Do About It – Complaint Handling Now*, in *Online Dispute Resolution: An International Business Approach to Solving* (2015) (describing how the threat of bad user reviews can help ensure compliance and explaining how chargebacks can facilitate dispute resolution).


2207 UNCTITAL, *supra* note 2201.

2208 Those procedures include a claimant submitting notice of a claim through an ODR platform; the parties negotiating through the ODR platform; if direct negotiations fail, then a neutral third-party is appointed to facilitate settlement; and if facilitated settlement fails, then the ODR administrator or neutral will inform the parties of the final stage of the process, which is left unspecified. *Id.* at 3.

2209 *Id.*


2211 *Id.*
the service, the parties’ EDCC must include a provision for the dispute to be resolved through Kleros court.\textsuperscript{2212} When creating the EDCC, the parties must agree upon choose how many jurors they want to determine the dispute, decide upon a court specialized in the topic of the contract, and deposit the necessary funds to enable the parties to use the service in the event of a dispute.\textsuperscript{2213} Additionally, the parties’ EDCC must specify the options available for the jurors to vote (e.g., reimbursement, additional time to complete the project).\textsuperscript{2214} Individuals from around the world self-select to serve as jurors using a token called a pinakion (PNK).\textsuperscript{2215} The probability of being drawn as a juror for a specific dispute is proportional to the amount of tokens the juror deposits. After assessing the evidence, jurors commit their vote to one of the options in the EDCC. Jurors are incentivized to vote honestly because once the dispute is over, jurors whose votes are not coherent with the group will lose tokens to those whose votes are.\textsuperscript{2216} A party can appeal the jury’s ruling by posting an additional appeal fee, and the dispute will be decided again by a jury containing twice as many jurors as the original plus one.\textsuperscript{2217}

**17.1.4.2 Distributed Jurisdiction**

Just as the Internet has changed how people interact with one another, the development of blockchain technology and EDCCs promises to yield an equally profound societal transformation. EDCCs may be able to govern online transactions but sometimes contain erroneous code or lead to unexpected results.\textsuperscript{2218} Also, while EDCCs can be coded to mitigate against many possible breaches, it is impossible to account for all of the instances where a breach may occur given the limitations of human behavior or incomplete information.\textsuperscript{2219} A lack of dispute resolution mechanisms to resolve these issues undermines the democratized and decentralized trust created by blockchain technology. The impossibility of consistently identifying parties to an EDCC conflict, combined with the difficulty of conceptualizing crypto problems, makes existing legal infrastructure inadequate for blockchain dispute resolution.\textsuperscript{2220} Instead, distributed open source ecosystems based on a concept of

\begin{itemize}
\item \textsuperscript{2212} Id.
\item \textsuperscript{2213} Id.
\item \textsuperscript{2214} Id.
\item \textsuperscript{2215} Id.
\item \textsuperscript{2216} Id.
\item \textsuperscript{2217} Id.
\end{itemize}
distributed jurisdiction and run through DApps or DAOs could provide a far more efficient and trusted resolution.

One such distributed jurisdiction is the Aragon Network Jurisdiction, the first DAO with the goal of acting as a governance system that allows organizations to build their businesses on the network and use the DAO’s decentralized arbitration system. The Aragon Network Jurisdiction defines a set of contracts to arbitrate disputes between parties, which serve as baseline rules for arbitrators. The contracts can be tailored to an individual organization’s jurisdiction through options for network token holders to vote on the EDCC’s initial terms.

The decentralized arbitration mechanism requires a party to a dispute to open a case and post a bond, which is locked for the period of the arbitration and returned if resolved in that party’s favor. If not, the bond is forfeited and kept as a network reserve. Five judges, selected from a pool of volunteers, are tasked with reviewing the rules and materials provided by the parties to the dispute. The judges then vote on the final judgment. If the party who posted the bond is unsatisfied with the “decentralized court” ruling, it can post a larger bond for another ruling, essentially moving up to a “court of appeals.” Finally, if the poster still finds the ruling unsatisfactory, it can appeal to the Supreme Court of the Aragon Network Jurisdiction, which will be composed of the top 9 judges ranked by Aragon Network Jurisdiction pay-out.

A distributed jurisdiction process such as this would be swift and efficient, with no requirement to consider subject matter or personal jurisdiction. Parties to the dispute could remain anonymous since the dispute resolution would be conducted on the blockchain, and the process should be handled quickly since it is completed online.

---


2223 Id.

2224 Id.

2225 Id.

2226 Id.

2227 Id.

2228 Id.

2229 Id.

Another potential decentralized dispute resolution process is the open source, intra-blockchain platform ecosystem proposed by Wulf Kaal. This system would allow parties to select arbiters, who make a determination then submit their judgments to the community for review and voting. Arbiters could become recognized for their subject matter expertise (through an open ledger displaying each arbiter’s decisions, as well as a rating system), allowing a party to request a specific category of arbiters. For individual users, such a system would be far easier to navigate than the traditional court system – and possibly easier to trust as well.\footnote{Kaal, \textit{supra} note 2219.}

### 17.2 Discovery – Third-Party Subpoenas

Enacted in 1986, Title II of the Electronic Communications Privacy Act\footnote{18 U.S.C. §§ 2701-2712.} prohibits certain providers of electronic communication services from disclosing the content of stored electronic communications to anyone except the owners of the communications.\footnote{18 U.S.C. § 2702(a).} The SCA prohibits the disclosure of such content even when requested pursuant to a valid subpoena.\footnote{Bower \textit{v. Bower}, 808 F. Supp. 2d 348, 350 (D. Mass. 2011); \textit{In re Subpoena Duces Tecum to AOL, LLC}, 550 F. Supp. 2d 606, 609-11 (E.D. Va. 2008).}

To establish an SCA defense, a subpoenaed third-party must establish that the service-providing entity was an electronic communication service available to the public and held the communication at issue in electronic storage as part of that service. An electronic communication service is statutorily defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications.”\footnote{18 U.S.C. § 2510(15).} Electronic storage is “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection.”\footnote{18 U.S.C. § 2510(17).} In one case, for example, allegations that “‘Dropbox keeps files in intermediate storage when users opt to share them’ and that [the plaintiff] keeps ‘backups’ of its ‘documents and files’ on Dropbox’s ‘cloud-based servers’” were sufficient to establish electronic storage of communications.\footnote{TLS Management \textit{v. Rodriguez-Toledo}, No. 15-2121 (BJM), 2016 WL 7413482, at *5 (D.P.R. Dec. 22, 2016).}

The SCA also protects the records of remote computing services under Section 2702(a)(2), stating that any person providing remote computing service to the public cannot divulge contents of any communication maintained on that service: A) “on behalf of, and received by means of electronic transmission from …, a subscriber or customer of such service;” and B) “solely for the purpose of providing storage or computer processing services to such subscriber or customer.”\footnote{18 U.S.C. § 2702(a)(2).}

Accordingly, a blockchain technology entity might successfully refuse to comply with a Rule 45 subpoena on grounds that it provides an “electronic communication service” and maintains
the communication in “electronic storage.” For example, a company providing a DApp that acts as a communication data repository, including the many blockchain instant messenger DApps such as Mercury Protocol, could invoke the SCA to protect user communications. Inevitably, most blockchain entities, such as DAOs, will integrate some method of communication, as most companies did with the creation of the Internet. Also, provided that the system stores communications instead of instantly erasing them like the messaging app Snapchat does, user communications would likely be protected by the SCA.

17.3 Authenticating Records Through the Blockchain for Evidentiary Purposes

The immutability of blockchain technology has the potential to facilitate the authentication of evidence at trial. Under the Federal Rules of Evidence, before a court can admit documentary evidence, “the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.” This authentication can be accomplished by direct or circumstantial evidence, including the testimony of a custodian of record, a knowledgeable witness, or an expert witness. With respect to Internet-based evidence, the type and quantum of evidence sufficient for authentication depends on the context and the court. For example, some courts have admitted online content as evidence based on witnesses whose testimony attributed the online content to the defendants. Courts have also allowed online evidence “authenticated
by a person's testimony that he is familiar with the online content and that the exhibits are in the same format as the online content.”

Since the purpose of the authentication process is essentially to ensure that the evidence is what the proponent claims it to be, blockchain technology can streamline this process. As information recorded on a blockchain is timestamped and distributed among computers on a decentralized network, blockchain-based records are nearly impossible to tamper with or alter. Thus, blockchain technology provides a degree of reliability, replacing the need for parties to call witnesses to authenticate documents, and thereby conserving judicial resources. Blockchain technology can also be submitted upon the sworn declaration of witnesses that the records were obtained from a blockchain, without the need for additional evidence to authenticate the document, thereby further enhancing judicial efficiency.

Despite these benefits, Congress has yet to enact a statute, and federal courts have yet to issue a new rule, permitting blockchain-based records to be admitted into evidence without further authentication. Nevertheless, one state has been proactive about allowing blockchain records to be authenticated without oral testimony. In 2016, Vermont enacted a statute concerning the authentication of records created using blockchain technology. Under the statute, a timestamped document on a blockchain “shall be considered a record of regularly conducted business” if:

- it is accompanied by a written declaration of a qualified person, made under oath, stating the qualification of the person to make the certification and: A) the date and time the record entered the blockchain; B) the date and time the record was received from the blockchain; C) that the record was maintained in the blockchain as a regularly conducted activity; and D) that the record was made by the regularly conducted activity as a regular practice.

The Vermont statute creates rebuttable presumptions that: “A fact or record verified through a valid application of blockchain technology is authentic”; “The date and time of the recordation of the fact or record established through such a blockchain is the date and time that the fact or record was added to the blockchain”; “The person established through such a blockchain as the person who made such recordation is the person who made the recordation”; and “[i]f the parties before a court or other tribunal have agreed to a particular format or means of verification

---

2245 United States v. Needham, 852 F.3d 830, 836 (8th Cir. 2017) (admitting screenshots of online content based on FBI agent’s testimony that he had viewed the online web pages and verified that the screenshots accurately represented those pages); United States v. Tank, 200 F.3d 627, 630 (9th Cir. 2000) (holding that a chatroom’s logs were authenticated by a witness’s testimony that he personally printed out the logs and that they accurately represented the chatroom conversations at issue); United States v. Standring, No. 1:04CV730, 2006 WL 689116, at *3 (S.D. Ohio Mar. 15, 2006) (permitting authentication of website printout by agent’s testimony combined with circumstantial evidence in the form of time-stamps and the web address).


of a blockchain record, a certified presentation of a blockchain record consistent with this section to the court or other tribunal in the particular format or means agreed to by the parties demonstrates the contents of the record."2248

17.4 Remedies – Valuation of Virtual Currency

When monetary relief is ordered and the asset in question is a virtual currency, courts are faced with the question of how much virtual currency must be paid. As virtual currency fluctuates in value, the price will likely change from the time of the events in the underlying dispute to the time litigation is initiated, to the time a judgment is rendered.

A Texas federal court addressed this issue in Securities and Exchange Commission v. Shavers,2249 holding that, for disgorgement purposes, a reasonable calculation in U.S. dollars could be obtained by multiplying the total amount of ill-gotten gains in bitcoin by the average daily price of bitcoin between the time the Ponzi scheme ended and the date of the court’s ruling.2250 Additionally, for the purposes of assessing civil penalties, which varied depending on whether the fraudulent act resulted in “substantial losses” to the victim, the court determined damages by multiplying the amount of bitcoin lost by the victims in the scheme with the currently available exchange rates.2251

In February 2016, a California bankruptcy court sidestepped this issue in an adversary proceeding where a liquidating trustee sued to recover the then-current value of 3,000 bitcoin ($1.3 million) paid by the debtor as commissions to an endorser of debtor’s mining product.2252 The trustee alleged that this was a fraudulent transfer and sought recovery pursuant to Section 550(a) of the Bankruptcy Code, which permits the trustee to recover, to the extent that a transfer of property is avoided, “the property transferred, or, if the court so orders, the value of such property.”2253 The endorser who had received the bitcoin argued it was currency under the Bankruptcy Code, which would have limited the trustee’s maximum potential recovery to approximately $360,000 (i.e., the value of the bitcoin at the time of transfer).2254 The court rejected

---


2249 In Shavers, the court granted the SEC’s motion for summary judgment on its claims against the defendants for violation of sections 5(a), 5(c), and 17(a) of the Securities Act of 1933, arising from the defendant’s operation of a bitcoin investment scheme. Sec. & Exch. Comm’n v. Shavers, No. 4:13-CV-416, 2014 WL 4652121, at *8-*9 (E.D. Tex. Sept. 18, 2014). Besides a permanent injunction, the court ordered disgorgement of $38,638,569 in profits (computed by multiplying the amount of ill-gotten bitcoin with the average daily price of bitcoin from the time that the scheme collapsed to the present time) with interest. The court further assessed penalties of $150,000 on each of the defendants for engaging in fraudulent misconduct that caused the loss of 265,678 bitcoin by investors, valued at $149 million at the time. Id. at *10-*11.

2250 Id. at *10.

2251 Id. at *11.


2253 Id.

2254 Id.
this argument on grounds that “bitcoin are not United States dollars,” but refrained from deciding whether the trustee should recover the actual bitcoin or its value because the trustee had yet to avoid the transfer.\textsuperscript{2255}

\textsuperscript{2255} \textit{Id.}
Comments and Suggested Corrections

All comments and suggested corrections, including broken links, should be directed to legal@blockchains.com.