Campbell Law Review

Volume 41
Issue 1 *Winter 2019*

Article 2

2019

The Lawyer's Cryptionary: A Resource for Talking to Clients About Crypto-Transactions

Carol Goforth

The Lawyer's Cryptionary: A Resource for Talking to Clients about Crypto-transactions

CAROL GOFORTH*

* University Professor and Clayton N. Little Professor of Law, University of Arkansas School of Law. Thanks to Cameron Brewer, my research assistant and a JD Candidate at the University of Arkansas School of Law, and to Associate Dean Will Foster and Professor Sharon Foster for their comments on earlier drafts of this article. Needless to say, any errors which remain are my own.

If you are anything like me, the first thing you heard about Cryptocurrency or crypto-technology was probably a vague reference to the Bitcoin "craze." That might have prompted some investigation, which could have led to the discovery that not millions, but billions of dollars were being invested in Cryptocurrencies of various sorts around the globe.[1]

1. As of May 2018, more than 1,600 Cryptocurrencies were being traded, and the total market capitalization for all of those Coins and Tokens was nearly $400 billion. *Top 100 Cryptocurrencies By Market Capitalization*, COINMARKETCAP, https://perma.cc/76YM-RNPU [hereinafter *Top 100 Cryptocurrencies*]. Some of the listed Coins and Tokens were essentially valueless, and some (like Bitcoin and Ethereum) had a capitalization worth billions of dollars. *Id.*

You might have wondered how people could possibly "value" something so intangible, often unrelated to any discrete asset, and lacking the promise of government backing. You might have been shocked at how that "thing" could have experienced such an increase in "value." Bitcoin, the world's first Cryptocurrency, went from being valued at less than a penny per Coin in May of 2010[2] to a sales price of $22[3] per Coin in February of 2013.[4] That alone seems remarkable, but the price of a single Bitcoin exceeded $19,000 in December of 2017.[5] In early May of 2018 it was trading at less than half of that, but a price of over $8,500 per Bitcoin[6] is still hard to comprehend for many.

In addition to stories about Bitcoin, those intrigued (or confused) by this alternative "currency" may have uncovered stories about the Securities Exchange Commission (SEC) halting trading in fraudulent and illegal Initial Coin Offerings (ICO)[7] and how the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) has been cracking down

2. This value is based on the first real world transaction involving Bitcoins, where 10,000 Coins were used to buy two pizzas in Florida. Eric Mack, *The Bitcoin Pizza Purchase That's Worth $7 Million Today*, FORBES (Dec. 23, 2013, 9:57 PM), https://perma.cc/E5E8-C2YU.

3. All references in this article are to U.S. dollars unless otherwise noted.

4. Sean Ludwig, *Y Combinator-backed Coinbase now selling over $1M Bitcoins per month*, VENTUREBEAT (Feb 8, 2013,12:03 PM), https://perma.cc/4B97-UKZN. Bitcoin and its origins are discussed in more detail later in this article. *See infra* Section II.3, II.12.1. The particular innovation that enabled Bitcoin to succeed involved consensus protocols that are described in more detail later in this article. *See infra* Section II.7, "Blockchain Consensus Protocols."

5. *Bitcoin Cash Charts*, BITCOIN.COM, https://perma.cc/W5JD-RECX.

6. On May 11, 2018, the trading price of Bitcoin was listed at $8,406.17 on the CoinDesk platform. *Bitcoin (USD) Price*, COINDESK, https://perma.cc/279A-WDVL (the value of Bitcoin over the past year can also be found here). To give you some idea of the volatility of Bitcoin pricing, on February 13, 2018, the opening price was $8,891.21. *Id.* On February 18, 2018, Bitcoin was trading at over $10,600.00. *Id.* The previously mentioned May 11, 2018, price was a "four day low" after Bitcoin had been trading at $9,357 on May 7. Omkar Godbole, *Bitcoin Risks Drop Below $9K After 4-Day Low*, COINDESK (May 8, 2018, 9:10 AM UTC), https://perma.cc/7K4A-NK7A. On August 15, 2018, Bitcoin's trading price was $6,270.04. *Bitcoin (USD) Price*, *supra* note 6.

7. Since late 2017, there have been several such notices. *See SEC Halts Alleged Initial Coin Offering Scam*, U.S. SEC. & EXCH. COMM'N (Jan. 30, 2018), https://perma.cc/W5BU-WDY9; *SEC Emergency Action Halts ICO Scam*, U.S. SEC. & EXCH. COMM'N (Dec. 4, 2017), https://perma.cc/PS24-SPMM; *Company Halts ICO After SEC Raises Registration Concerns*, U.S. SEC. & EXCH. COMM'N (Dec. 11, 2017), https://perma.cc/X2XN-BXDN.

on illicit "financial practices" involving Virtual Currencies.[8] Those curious about the phenomenon may also have read stories about investors who have lost hundreds of millions of dollars in value because of hacks, poor security, and outright fraud.[9] Many probably have also seen references to the "revolutionary" Blockchain technology at the heart of these new Cryptocurrencies and Cryptokens, along with brave pronouncements that this technology has "the potential to revolutionize the world economy."[10] Many observers are likely to be intrigued by businesses that have accepted or are considering accepting cryptocurrencies,[11] and how major corporations are turning to Blockchain technology in a variety of contexts.[12] The Uniform Law Commission recently promulgated a model act for states concerned about the need to regulate Virtual Currency businesses.[13] In a growing number of states, there have been other legislative or regulatory reactions to the spread of Virtual Currencies.[14] A recent ethics opinion even limits circumstances under which it is appropriate for lawyers to accept Cryptocurrencies as their fee for

8. *E.g.*, *FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales*, FIN. CRIMES ENF'T NETWORK (July 17, 2017), https://perma.cc/R8P3-63DZ.

9. At least one source claims that Bitcoin investors alone have lost about $15 billion over the lifetime of the currency. Steven Melendez, *Bitcoin Heist Adds $77 Million To Total Hacked Hauls Of $15 Billion*, FAST CO. (Dec. 7, 2017), https://perma.cc/BTP3-VQA8.

10. Don Tapscott et al., *How Blockchains Could Change the World*, MCKINSEY & CO. (May 2016), https://perma.cc/84H8-Z9R2.

11. Domino's Pizza, Expedia, Lionsgate Films, Overstock, Microsoft, Save the Children, Tesla, Shopify, Subway, Whole Foods, and Zynga are among the companies that currently accept Bitcoin. Jonas Chokun, *Who Accepts Bitcoins As Payment? List of Companies, Stores, Shops*, 99 BITCOINS (Aug. 20, 2018), https://perma.cc/28TT-TX72.

12. As one source describes,

> Almost six in 10 large corporations are considering using blockchain, according to a Juniper Research survey of 400 executives, managers and tech staff. The technology is increasingly being tested or used by companies such as Wal-Mart Stores Inc. and Visa Inc. to streamline supply chain, speed up payments and store records.

Bloomberg, *Blockchain Is Pumping New Life Into Old-School Companies Like IBM and Visa*, FORTUNE (Dec. 26, 2017), https://perma.cc/VJ99-WTT9.

13. UNIF. REGULATION OF VIRTUAL-CURRENCY BUS. ACT (UNIF. LAW. COMM'N 2017) [hereinafter UNIF. ACT]. This Act was approved by the ULC at its annual meeting in July 2017 and was published October 9, 2017. *Id.* As of the date this article was written, the Act had been introduced in both Hawaii and Nebraska. *Regulation of Virtual-Currency Businesses Act: Legislative Tracking*, UNIF. LAW COMM'N, https://perma.cc/EQ2T-MHDG.

14. For example, the New York Department of Financial Services has chosen to regulate Virtual Currencies. *See* N.Y. FIN. SERV. LAW § 200 (2017).

services.[15] With these rapid and confusing developments, lawyers may be concerned that if a client or prospective client walks into their office and wants to talk about any of this, they won't know enough to even understand what the client is talking about.

This introductory article is, therefore, designed to help by providing a list of terms and explanations to introduce lawyers to various basic concepts related to Cryptocurrencies and Blockchain. The goal of this article is to help lawyers communicate intelligently with clients who want to understand whether they can realistically attempt to raise funds by issuing some of these Tokens, whether they should accept Cryptocurrency as payment for goods or services, whether they or their companies can legally invest in cryptoassets, or how the current regulatory framework is likely to apply to cryptotransactions. The goal of this article is not to turn readers into experts with regard to any of the myriad legal issues that might follow, such as whether a transaction will involve the issuance or purchase of a security, will be regulated by the Commodity Futures Trading Commission, will have particular tax consequences, or will trigger reporting requirements under banking laws and regulations. This article certainly does not consider the additional ramifications of international transactions. All of these issues require particular expertise, which will undoubtedly require additional research and information. Instead, this is intended to act as a Cryptocurrency dictionary (a "cryptionary") rather than a more traditional exposition of the law relating to a given topic. Part I discusses the organization of the article. Part II contains an alphabetized listing of thirty-seven distinct terms relating to Cryptocurrencies along with definitions and explanations of those concepts. Part III concludes with a very brief overview of some of the most important regulatory issues that may be relevant before an attorney offers legal advice relating to Cryptocurrencies or other cryptoassets.

I. ORGANIZATION OF ARTICLE

Because this article is intended to serve as a "cryptionary," it contains an alphabetical consideration of terms that are important to understanding

15. Debra Cassens Weiss, *Lawyers Can Accept Payment in Bitcoin, Nebraska Ethics Opinion Says*, A.B.A. J. (Sept. 18, 2017), https://perma.cc/JA67-4HT3. The caveat is that while lawyers can accept digitals currencies like Bitcoin, they "must immediately convert the money into U.S. dollars." *Id.* This is required under Nebraska law to "assure that the fee charged remains reasonable." *See Nebraska Ethics Advisory Opinion for Lawyers No. 17–03* (Sept. 11, 2017), https://perma.cc/2YRV-5SGY.

Cryptocurrencies and cryptotransactions.[16] The importance of the different concepts discussed here depends too much on context for any other organizational scheme to be effective, whereas alphabetizing the various words and phrases has the benefit of making these terms easier to search. There are a couple of exceptions to this general organizational framework.

First, because the word "Cryptocurrency" is used throughout this article, and because the concept is so foundational, a brief explanation is provided here.[17] In its broadest sense, Cryptocurrency is a term that has been used to refer to all digital interests that operate like currency, are secured using cryptography, and operate on a peer-to-peer basis independent of any third party intermediary, including any governmental authority.[18] If you break this statement down, the requirements include: (i) a digital interest, (ii) operating like a currency, (iii) using cryptography, (iv) on a peer-to-peer network.[19] A digital interest is obviously one that is represented without a physical token, such as a tangible note or coin, and instead exists only in electronic format.[20] In order to operate as a currency, the digital interest needs to have one of the generally accepted attributes of currency, such as acting as a medium of exchange, a store of value, or a unit of account.[21] In order to be a Cryptocurrency, ownership of the

16. Many of the words discussed here are terms of art, and are, therefore, sometimes capitalized in the available literature. Because this article is written for lawyers, and a common convention in legal contracts is to capitalize defined terms, that is what this article does, even though the capitalization is not always what cryptographers or Cryptocurrency experts are used to seeing or using. The terms that are explained in this article are generally capitalized throughout, which means that if you see an unfamiliar word or phrase and it is capitalized, there is likely to be a more detailed explanation of that language in the numbered definitions in Part II of this article.

17. There is also a more complete explanation of Cryptocurrency in Section II.12 of this article. That definition also includes a series of examples which are in separately numbered sections. The second instance in which this article deviates from an alphabetical listing of terms involves the definition of "Token," which is a term often used to refer to a particular kind of cryptoasset. Tokens are discussed (in summary fashion) in this section of the article, as well as having a more complete definition in Section II.34.

18. *See, e.g.*, Martin Tillier, *What is a Cryptocurrency?*, NASDAQ (Jan. 25, 2018, 10:58 AM) (on file with Campbell Law Review).

19. *Id.*

20. It has long been possible to transfer funds without using any physical form of money. Checks, for example, allow a bank to transfer money from one person's account to another through the simple expedient of updating a ledger. Debit cards allow the same thing to occur entirely electronically. *Id.*

21. This definition is consistent both with traditional definitions of such words as money and currency, and also with more modern statutory and regulatory definitions of Virtual Currency. (For a more complete discussion of Virtual Currency, see Definition 36 in Part II of this article.) Money is "something generally accepted as a medium of exchange, a measure of value, or a means of payment . . . ." *Money*, MERRIAM-WEBSTER,

interest needs to be secured against theft by cryptographic means.[22] Finally, transactions involving the transfer of ownership would not be overseen by a bank, a government, or any third party charged with maintaining a ledger of ownership; instead, the only parties involved in authenticating the ownership and transfer of the interest would be the users of the interests.[23]

This last element deserves more attention. What is the significance of having this kind of user network? Consider how a bank oversees the movement of money between accounts. You deposit money and the bank acts as the intermediary, keeping a record of how much you have deposited. You authorize a payment to someone else, and the bank records a withdrawal from or debit to your account and a corresponding payment or credit to the payee's account. This transaction is recorded by the bank on the bank's ledger.[24] In the same way, a stock ledger records ownership and transfer of ownership of stocks, and a real estate ledger records ownership

---

https://perma.cc/GT7A-UGB2. Currency is defined by the same source as "a medium of exchange." *Id.* Oxford Dictionaries defines money as a "current medium of exchange . . . " and currency as "[a] system of money in general use in a particular country." *Money*, OXFORD DICTIONARIES, https://perma.cc/RZ7C-UZWP; *Currency*, OXFORD DICTIONARIES, https://perma.cc/2W9R-KQEJ.

The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) defines "Virtual Currency" to be "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency." U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (MAR. 18, 2013). Virtual currency is defined in the Uniform Law Commission's Uniform Regulation of Virtual-Currency Business Act (2017) as "a digital representation of value that: (i) is used as a medium of exchange, unit of account, or store of value; and (ii) is not legal tender, whether or not denominated in legal tender . . . ." UNIF. ACT§ 102(23), *supra* note 13, at 17 (exclusions omitted). The Conference of State Bank Supervisors (CSBS) has similarly determined that, for its purposes, "Virtual Currency is a digital representation of value used as a medium of exchange, a unit of account, or a store of value, but does not have legal tender status as recognized by the United States Government." CONFERENCE OF STATE BANK SUPERVISORS, STATE REGULATORY REQUIREMENTS FOR VIRTUAL CURRENCY ACTIVITIES, 2 (SEPT. 15, 2015); *see also* N.Y. FIN. SERV. LAW § 200 (2017) (similar definition as part of the N.Y. BitLicense requirements).

22. Cryptography is simply computer code that allows information to be kept secret by virtue of transmitting it in an unrecognizable format until an appropriate mechanism is employed to decode the data. *See Cryptography*, TECHNOPEDIA, https://perma.cc/P2PY-UWT5. The very word "Cryptocurrency" was derived from combining cryptography with currency. *See* Tillier, *supra* note 18.

23. *See* Tillier, *supra* note 18.

24. Richard G. Brown, *A Simple Explanation of How Money Moves Around the Banking System*, RICHARD GENDAL BROWN BLOG (Nov. 24, 2013), https://perma.cc/JFA4-8QSD. This is obviously an over-simplified explanation.

and transfer of title to real estate. In each case, there is a centralized authority charged with maintaining the appropriate records or ledger.

In a peer-to-peer network, the ledger is digital and decentralized or, in other words, distributed electronically to all the users or participants. This means that the entire record of ownership from the time the network is created is held by all users. Because all the records are digital, every computer in the network will have access to all information regarding the entire chain of ownership of all of the assets in that network.[25] "In effect, it is the users themselves and their vast combined computing power that record transactions directly between peers, rather than through banks or other intermediaries. That system is known as a [B]lockchain and the transactions, and even the currencies, are sometimes referred to as 'peer-to-peer.'"[26] Blockchain refers both to the chain of information and to the process by which each user in the peer-to-peer network can be assured that any given transaction is valid.[27]

The underlying Blockchain technology has many potential applications beyond the issuance of interests that are intended to serve as a replacement for conventional currencies.[28] Because the first successful use of Blockchain was Bitcoin,[29] the notion that the law needs to regulate such interests as Cryptocurrencies seems to have dominated legal discourse.[30] Efforts to distinguish certain kinds of interests as Tokens,[31] instead of

25. The actual identities of individual participants are kept secure through the use of Cryptographic Hashing (*see infra* Section II.13) and the Public and Private Keys (*see infra* Section II.25) for each user.

26. Tillier, *supra* note 18.

27. "Blockchain" is defined in greater detail in Section II.5 of this article.

28. For example, one recent article lists the following 20 uses for Blockchain beyond Bitcoin: (1) payment processing and money transfers; (2) to monitor supply chains; (3) for retail loyalty rewards programs; (4) as digital IDs; (5) for data sharing; (6) for copyright and royalty protection; (7) for digital voting; (8) real estate, land, and auto title transfers; (9) food safety; (10) immutable data backup; (11) tax regulation and compliance; (12) for workers' rights; (13) medical recordkeeping; (14) weapons tracking; (15) wills and inheritances; (16) equity trading; (17) managing internet of things networks; (18) expediting futures trading and compliance; (19) securing access to belongings; and (20) tracking prescription drugs. Sean Williams, *20 Real-World Uses for Blockchain Technology*, MOTLEY FOOL (Apr. 11, 2018, 9:21 AM), https://perma.cc/JT54-A8YU.

29. Bitcoin is discussed further both in Section II.3 and Section II.12.1, as an example that serves as part of the Definition for Cryptocurrency.

30. There is sometimes confusion about whether the interests should be called Cryptocurrencies or Virtual Currencies, or indeed broken down into different categories. The expanded consideration of Cryptocurrency in Section II.12 and the definition and discussion of Virtual Currency in Section II.36 may be helpful in clarifying this issue.

31. *See infra* Section II.34.

Coins,[32] or as utility Tokens,[33] instead of Tokens subject to regulation as securities,[34] have therefore not been very successful.[35] Almost any digital asset (regardless of how the creator intends it to function or hopes to market it) could serve as a medium of exchange or a store of value or a unit of account; under current rules this means that it is at least somewhat like a currency.[36] In addition, regardless of the creator's intentions, if a cryptoasset is viewed by purchasers as a speculative investment or is used to fund terrorism or launder funds or fund illegal activities, regulators will act, potentially in ways that also impact the most legitimate of businesses.

The second exception to the organizational framework of this article applies to the generally accepted definition of "Token."[37] Tokens themselves can be classified in many different ways.[38] This article suggests a way of looking at Tokens from the perspective of a lawyer

32. *See infra* Section II.8.

33. A "utility" Token is supposed to be a Token that has some functional utility beyond merely serving as a currency. *See* Iyke Aru, *The Fundamental Principles of Utility Tokens in the Blockchain Ecosystem*, CCN (March 4, 2018), https://perma.cc/WJ3C-49U6. Some commentators tried to suggest that such interests should not be regulated like true Cryptocurrencies, and should not even be securities. For example, the entire thought process behind the Simple Agreement for Future Tokens (SAFT) (*see infra* Section II.30) was that functional utility Tokens should not be regulated as securities. *See infra* notes 280–90 and accompanying text. The SEC, however, has soundly rejected this argument, explicitly stating that it intends to exercise its jurisdictional powers over the sales of cryptoassets regardless of whether a particular transaction involves a so-called utility Token. Joseph Young, *SEC Hints at Tighter Regulation for ICOs, Smart Policies for "True Cryptocurrencies,"* COINTELEGRAPH (Feb. 9, 2018), https://perma.cc/NJP7-L5LT.

34. For a discussion of Tokens as securities, see Section II.34, and particularly II.34.4.

35. For example, the Commissioner of the SEC has repeatedly asserted, without equivocation, that "ICOs are securities offerings that must be either registered with the SEC or qualify for a private placement exemption." Michael H. Krimminger et. al., *SEC and CFTC Testimony on Virtual Currencies: Is More Regulation on the Horizon?*, CLEARY FINTECH UPDATE (Feb. 14, 2018), https://perma.cc/RD6U-G9TW; *see also Statement on Cryptocurrencies and Initial Coin Offerings*, U.S. SEC. & EXCH. COMM'N https://perma.cc/VS37-B475.

36. *See* Tillier, *supra* note 18.

37. *See infra* II.34.

38. One commentator, for example, proposed looking at Tokens along five specified dimensions: their technical layer, their purpose, the utility to which the Token can be put, the legal status of the Token, and their underlying value. Thomas Euler, *The Token Classification Framework: A Multi-dimensional Tool for Understanding and Classifying Crypto Tokens*, UNTITLED INC. (Jan. 18, 2018), https://perma.cc/6CCL-Q8BW. This approach produced more than a dozen distinct categories of Tokens. *Id.* Another source proposed looking at such interests to determine whether they were useful as a store of value, for network utilization, as the equivalent of an equity interest, or whether they were pegged to other assets. Basiccrypto, *Is Your Crypto Digital Gold, Gas, or Something Else?*, STEEMIT BETA. https://perma.cc/WJG7-6ER2.

interested in predicting what kinds of regulatory regimes are most likely to be applicable. Because this is an area in which regulation is rapidly evolving, the categories mentioned here are necessarily broad and somewhat amorphous. In addition, the categories overlap since Tokens can have multiple functions and because regulatory agencies can certainly have overlapping jurisdiction.[39]

With this background in mind, specific terms can be explained and discussed in more detail.

II. TERMINOLOGY[40]

1. Address (Cryptocurrency Address)

Cryptocurrency Addresses, which typically present as a string of alphanumeric characters, are used to send or receive information about transactions on a network in the same way that an internet protocal (IP) address routes communications on the internet. In fact, when Bitcoin was first presented to investors, it was possible to send Coins to IP addresses, but developers realized that this could result in man-in-the-middle attacks.[41] Therefore, this approach was quickly abandoned. Now, the applicable Address to which a transaction is sent will be based on a series of cryptographic algorithms that present the Public Key in a readable way designed to prevent typographic errors. The technical details of Addresses are far beyond the scope of this article, but it is important to know that current configuration of Addresses generally ensures that they are relatively

39. *See infra* Section II.34.

40. Note that the terminology discussed in this article may not always coincide with a client's usage. Certain terms are used differently by different individuals. One recent source, for example, in commenting on the difficulty in understanding the difference between Coins and Tokens, specifically noted that "[t]he terms 'coins' and 'tokens' are confusing and are interpreted differently by different individuals." *Difference Between Cryptocurrency Coins and Tokens,* CRYPTONIAM (Dec. 5, 2017) (italics omitted), https://perma.cc/9A4W-V77P. Where possible, this article attempts to adopt what appears to be the most widely accepted technical usage and understanding of terms as of the date this material was written.

41. Ameer Rosic, *Blockchain Address 101: What Are Addresses on Blockchains?* BLOCKGEEKS, https://perma.cc/7WW4-ZWQE. A "man in the middle attack" occurs "when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway." *Man in the Middle (MITM) Attack,* IMPERVA INCAPSULA (on file with Campbell Law Review). IP addresses are relatively accessible; current wallet addresses are not. By way of example, a Bitcoin Wallet address might be something like: 1PMzaLrc8jjyQbkQtNuYUWiQX9p6dkxnoz.

easy to use,[42] and they provide the starting point for making sure that transactions are secure and cannot be disrupted by third parties.[43]

2. Altcoin

"Altcoin" is the general term for Cryptocurrencies that are specifically designed as alternatives to Bitcoin. Most of these promote themselves as better than Bitcoin in one or more ways and were launched after the initial success of Bitcoin.[44] This general term includes a wide variety of Cryptocurrencies that have special attributes in addition to being a potential medium of exchange, unit of account, or store of value. Altcoins may possess a range of utility or functionality. For example, they may have specific applications for particular platforms; they can serve as developer tools; they can provide a means or mechanism for sharing data; they may offer improved protocols for establishing authenticity; or they may offer increased privacy and sovereignty.[45]

3. Bitcoin

A consideration of "Bitcoin" is important because of the dominating space Bitcoin occupies in the crypto and financial worlds.[46] Bitcoin is a digital or Virtual Currency that was launched in 2009 when the Bitcoin network went public, making Bitcoin available to anyone who successfully

42. They are safe to send and free to create; most sources suggest sending a new address for every transaction in order to prevent third parties from being able to predict your monetary habits. *See Bitcoin Addresses*, LEARN CRYPTOGRAPHY, https://perma.cc/7H5F-W535.

43. For a more detailed explanation of all of this, see Rosic, *Blockchain Address 101*, *supra* note 41. You will note that the text talks about a "Public Key." *Id.* To actually send and receive cryptographic assets, a user must have both a Public and Private Key. *Id.* Think about a Public Key as being a little bit like an email address: both the owner of the email account and others can see that address. A Private Key is like the password; it is a secret known only to the owner of the account. The combination of Public and Private Keys help keep cryptographic transactions secure. For some of the limitations on the accuracy of this simile, *see infra* note 260. Keys are explained further in Section II.25.

44. *Altcoin*, INVESTOPEDIA, https://perma.cc/73ZG-NWU2.

45. For a laundry list of possible uses for Tokens created with Blockchain technology, see *Cryptographic Tokens*, BLOCKCHAIN HUB, https://perma.cc/349B-FSNA (listing possibilities such as serving as a "Token of ownership; Voucher to redeem for physical items on platforms that only permit the sale of digital goods; Software license; Stock certificates; Access rental cars or other vehicles; Ticket or access pass (party, concert, amusement park, ect. [sic]); Automated road and bridge tolls"; etc.).

46. For a further description of Bitcoin, *see infra* Section II.12.1.

"Mined" it.[47] In contrast to traditional government-backed currencies ("Fiat"),[48] Bitcoin "has no central[ized] bank, nation state, or regulatory authority backing it up."[49] "Bitcoins" have no tangible existence and instead are balances in the Blockchain ledger, controlled by digital Keys stored in a digital Wallet that can exist online or on an investors' own hardware.[50] As of May 15, 2018, the total capitalization of Bitcoin was just over $146 Billion.[51] This is not to say that Bitcoin is universally applauded. The vice-chairmen of Warren Buffett's investment firm Berkshire Hathaway recently called it a "totally asinine" "noxious poison."[52]

Nonetheless, as the first successfully established Cryptocurrency, Bitcoin has been the "de facto standard" for all Cryptocurrencies.[53] The technological foundation for Bitcoin was first publicized in 2008 in a paper entitled *Bitcoin—A Peer to Peer Electronic Cash System* and originally posted in an online discussion of cryptography.[54] It was posted under the pseudonym Satoshi Nakamoto, whose real identity still remains a mystery.[55] The paper presented the innovative idea of consensus protocols in the form of Proof-of-Work, which provides a solution to the issue of

47. Mining is defined *infra* Section II.26. The first, or genesis, Block was mined on January 3, 2009, by the person or persons using the pseudonym Satoshi Nakamoto. *Genesis Block*, INVESTOPEDIA, https://perma.cc/V22A-K5PZ.

48. "Fiat" is Latin for "it shall be," and although technically it could refer to any medium of exchange not tied to something with tangible value, it has come to refer to "money" or "currency" that has value because a government has decreed that it does. Neale Godfrey, *A Few Words About Bitcoin . . . Because Fiat is Not Just a Car*, FORBES (Mar. 8, 2015, 8:40 AM), https://perma.cc/SS6J-C4NB.

49. Julia Finch, *From Silk Road to ATMs: The History of Bitcoin*, THE GUARDIAN (Sept. 14, 2017, 2:21 PM), https://perma.cc/VWL2-K923.

50. *How do Bitcoin Transactions Work*, COINDESK (Jan. 29, 2018), https://perma.cc/RBG5-FUYN.

51. *Top 100 Cryptocurrencies*, *supra* note 1.

52. Julia Kollewe, *Bitcoin is 'noxious poison', says Warren Buffett's investment chief*, THE GUARDIAN (Feb. 15, 2018), https://perma.cc/7N6G-92VW.

53. sajalali, *The Six Most Important Cryptocurrencies Other than Bitcoins*, STEEMIT BETA, https://perma.cc/A53S-UT6S. While Bitcoin may be the most influential, it was not the first attempt to create digital currency with an encryption-secured ledger. Bernard Marr, *A Short History Of Bitcoin And Crypto Currency Everyone Should Read*, FORBES (Dec. 6, 2017, 12:28 AM), https://perma.cc/KMJ7-GT9N (offering both B-Money and Bit Gold as examples of formulations that were never fully developed).

54. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN, https://perma.cc/ZUV2-LZHL.

55. Mark Hodge, *CRYPTO CREATOR Who is Satoshi Nakamoto? Bitcoin creator whose identity is unknown but could be one of the richest people in the world*, THE SUN (Feb. 12, 2018, 7:30 PM), https://perma.cc/KYL6-QTU3 (describing the unsuccessful efforts at identifying him (or them)).

how consensus can be reached as to the validity of transactions on a decentralized network absent the ability to trust the other parties who are involved.[56]

Given both the speed with which Bitcoin has risen to prominence (far outpacing effective regulation and oversight) and the sheer amount of money involved, it is not surprising that there have been bumps along the way. For example, in 2011, MyBitcoins, a Wallet service, suddenly disappeared from the web, reportedly because the site was hacked.[57] In 2012, Bitcoinica, an early Bitcoin Exchange, was hacked multiple times before being closed, and several other Exchanges were also shut down.[58] In January 2014, the world's largest Bitcoin Exchange at the time, Mt. Gox, suddenly declared bankruptcy and 850,000 Bitcoins (then valued at approximately $460 million) were apparently lost to hackers.[59] Hackers continued to exploit weaknesses in Bitcoin Exchanges in 2015 and 2016.[60]

However, these insecurities all relate to sites that trade in or host ownership of Bitcoin; the Decentralized Blockchain Ledger technology, which underlies the success of Bitcoin, has proven to be remarkably secure and successful.[61] Certainly, clients that come in wanting to talk to an attorney about Cryptocurrencies or Tokens will expect more than a knee-

56. Nakamoto, *supra* note 54, at 3. For a discussion of consensus protocols, see Section II.7. For an even more detailed discussion of the problem of consensus for decentralized networks, see Ameer Rosic, *Basic Primer: Blockchain Consensus Protocol*, BLOCKGEEKS, https://perma.cc/NXH5-GQDA.

57. Timothy B. Lee, *WATCH OUT—A Brief History of Bicoin Hacks and Frauds*, ARS TECHNICA (Dec. 5, 2017, 7:30 AM), https://perma.cc/5NGT-WKSC. Wallet services were typically advertised as a convenience to investors, supposedly allowing investors to store their Coins or Tokens on the Wallet service site. Unfortunately, lacking regulation, there was no way to see if the service was truly secure. Not surprisingly, when the MyBitcoins site went down, the developers blamed hackers. *Id.*

58. *Id.*

59. Robert McMillan, *The Inside Story Of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014, 6:30 AM), https://perma.cc/QM4E-PFZR. At the time, it was handling roughly 70% of Bitcoin trading. Paul Vigna, *5 Things About Mt. Gox's Crisis*, WALL ST. J. (Feb. 25, 2014, 2:03 PM), https://perma.cc/TEU6-BD9Z. This hack caused the price of Bitcoin to plummet from $660 to below $200 over the next year. *Id.*

60. In January 2015 Bitstamp was hacked for approximately $5 million, and in August of 2016 Bitfinex announced the loss of $77 million. Nathaniel Popper, *Warning Signs About Another Giant Bitcoin Exchange,* N.Y. TIMES (Nov. 21, 2017), https://perma.cc/33T3-5DG8. Both of these exchanges still exist, although Bitfinex in particular has been criticized as being opaque, and "provid[ing] no information on its website about where it is or who operates the company." *Id.*

61. As one source has noted, "[a]ll of the thefts in recent years have been the result of carelessness on the part of bitcoin owners, or else incompetency or dishonesty from the companies they used." Jeff John Roberts, *How Secure Is Bitcoin Really?*, FORTUNE (Dec. 9, 2017), https://perma.cc/Q2CS-K9YC.

jerk reaction that the technology is not secure. The economic success and longevity of Bitcoin has at least proven that its underlying technology is workable and can be reliable.[62] Its history also proves that service providers who offer platforms on which such Coins can be stored or traded may not be as secure, and that there are potential risks with investment in or utilization of Virtual Currencies. In addition, clients interested in providing services that relate to Cryptocurrencies should be aware that the regulatory framework in this country is rapidly evolving.[63]

4. Block

In the context of Blockchains, a "Block" is a permanently recorded, time-stamped transaction aggregated with other transactions that occurred at about the same time.[64] One of the simplest ways to think about this is as if a "Block" is the equivalent of a page in a ledger or record book.[65] Each Block will also contain a reference to the immediately preceding Block (so that the system knows where it is to be placed in the chain) and a difficult to solve mathematical puzzle.[66] The problem in the Block must then be solved before the next Block can be added to the chain.[67] This is necessary so that the Blocks are added to the chain (the "Blockchain") in the same sequence by everyone in the network. The first transaction in each new Block is the genesis transaction, and it will contain the record of which addresses or scripts are entitled to receive the reward for solving the

62. When originally issued, Bitcoin was regarded with a great deal of skepticism. One noted source suggested that "the uses of bitcoin as a medium of exchange appear limited, particularly if one excludes illegal activities." François R. Velde, *Bitcoin: A Primer*, 317 CHI. FED. LETTER 4 (Dec. 2013) (on file with Campbell Law Review). On the other hand, even this commentator acknowledged that it represented "a remarkable conceptual and technical achievement[.]" *Id.* Today, however, although various wallet and exchange services have been hacked and suffered various failures, Bitcoin itself is still going strong according to its original coding, and Blockchain technology has proven to be remarkably versatile. *See supra* notes 28 and 45 for various applications of Blockchain technology.

63. *See, e.g.*, *infra* Section II.35, and notes 354–93 and accompanying text describing the regulatory situation in the United States; *see also* Sarah Jane Hughes & Stephen T. Middlebrook, *Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries*, 32 YALE J. ON REG. 495, 559 (2015) [hereinafter *Advancing*] (discussing potential avenues for the regulation of Cryptocurrencies).

64. *Block (Bitcoin Block)*, INVESTOPEDIA, https://perma.cc/6TE7-3VX6.

65. *Id.* These illustrative examples also appear in the *Block*, BITCOIN WIKI, https://perma.cc/RQH4-HQ9K.

66. *Block (Bitcoin Block)*, *supra* note 64.

67. *Id.*

mathematical problem.[68] Because each Block begins with the reference to the prior Block, and in turn contains a problem that must be solved in order for the next Block to be added, the sequence of Blocks essentially forms a chain. However, it is possible for the chain to have temporary splits or Forks,[69] which would happen, for example, if two computers performing Mining[70] operations coincidentally arrive at two different valid solutions for the same Block at the same time. The peer to peer network[71] is designed to resolve these splits within a short period of time, so that only one branch of the chain survives.[72] The surviving chain is the one with the most combined difficulty.[73]

5. *Blockchain*

First utilized in 2008 in connection with the development of Bitcoin, Blockchain is a technological and cryptographic process involving a digital decentralized ledger in which transactions are added in chronological order, creating a "chain" of Blocks. The information held on that distributed chain is continually being updated and reconciled.[74] Because the information is shared in its entirety among so many computers (i.e., it is

68. It is this reward that supports the practice of Mining. Mining is further discussed in Section II.26 of this Article.

69. *See infra* Section II.22 for discussion of Forks.

70. *See infra* Section II.26 for discussion of Mining.

71. *See supra* notes 23–26 and accompanying text for a description of what is meant by peer-to-peer transactions.

72. Consider this scenario:

> When miners mine for proof-of-work and land a valid block, there is a chance that two miners would get a valid block somewhat at the same time (when I say "somewhat" I mean when a miner successfully finds a block and broadcasts that to other nodes, some other node get the block and distribute it before receiving the successful block). So when two nodes get a valid block simultaneously a fork happens. Say the two valid blocks are A and B.
>
> Now the blockchain will resume on the next found block. Some miners are mining on A others are mining on B; the chain that hits the next block first C will be the main chain, given it will be the longest. It rarely happens that the forks extends more than 4 blocks.

Explain Forks & Hard and Soft forks to me, VERIFY.AS (Oct. 23, 2017), https://perma.cc/M7NY-V9FW.

73. This is to prevent someone from creating a split or Fork in the chain and rapidly creating a large number of low-difficulty Blocks that it is programmed to solve, thereby having it accepted by the network as "longest." For a discussion of Hard and Soft Forks, see *infra* Section II.22.

74. The ledger is decentralized because it is distributed to a network of computers rather than being held in one central location. For a description of the process by which Blocks are reconciled, see *infra* Section II.7 describing Blockchain Consensus Protocols.

wholly distributed), it cannot be controlled by any single entity, and the system therefore has no single point of access where a hacker or other outside force can interrupt or corrupt the information on the chain. It is protected from being corrupted because altering any unit of information on the Blockchain would mean using a huge amount of computing power to override the entire network.[75] Blockchain technology therefore allows digital information to be distributed but not altered unilaterally.[76]

6. *Blockchain 2.0*

As one might expect with new technology, there have been a wide variety of developments relative to the use and utility of Blockchain technology. Originally conceived as a vehicle with the potential to act as a medium of exchange, Blockchain has evolved into a platform for other innovations. The expanded functionality is sometimes called "Blockchain 2.0."[77]

In essence, while Blockchain was originally designed to support applications involving Cryptocurrencies,[78] Blockchain 2.0 allows for programmable transactions, which are transactions dependent on a condition or a set of conditions. Blockchain 2.0 therefore creates a range of new economic opportunities previously unavailable on the web, including such things as microtransactions, decentralized exchange, and Smart Contracts.[79] Smart Contracts, which are scripts executed in the context of a Blockchain, are defined in greater detail in Definition 32.[80]

---

75. "The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value." Ameer Rosic, *What is Blockchain Technology? A Step-by-Step Guide For Beginners*, BLOCKGEEKS (2017), https://perma.cc/T747-YZ4D (quoting DON & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION (2016)).

76. *Id.*

77. Roman Alyoshkin, *Blockchain 2.0 The Purpose of Blockchain*, POLYS BLOG (Oct. 3, 2017), https://perma.cc/KC4Y-HWMM.

78. Martin von Haller Gronbaek, *Blockchain 2.0, Smart Contracts and Challenges*, BIRD & BIRD (June 16, 2016), https://perma.cc/VV7L-JKHS.

79. Alyoshkin, *supra* note 77, at 2.

80. *See infra* Section II.32. One way of looking at smart contracts is to break them into their constituent components. In this light, they are (1) pre-programmed logic written in computer code, (2) stored and replicated on a distributed platform or Blockchain, (3) that is then executed or run by a network of computers (typically the same computers that host the Blockchain), (4) which then results in ledger updates pursuant to the terms of the agreement as specified in the computer code. Antony Lewis, *A Gentle Introduction to Smart Contracts*, BITS ON BLOCKS (Feb.1, 2016), https://perma.cc/K2VG-C9K4. Another way of looking at it is to focus on the overall context: "a smart contract enforces a relationship with

7. Blockchain Consensus Protocol

Presumably, any attorney relying on this kind of article to provide a background into Blockchain and Cryptocurrencies will not be expected to provide technical operational advice to clients.[81] Nonetheless, it is conceivable that clients will expect attorneys providing general advice about regulatory requirements (either those in place or those that might be proposed in the foreseeable future) to understand how the various Consensus Protocols can be used to provide assurance of security and platform reliability.[82]

Before Bitcoin, efforts at establishing peer-to-peer decentralized currency systems failed because they were unable to answer the problem that had come to be called the "Byzantine Generals Problem."[83] That problem has been described like this: suppose that in a world before mobile communications, several army groups surround a castle they hope to conquer. Only a simultaneous attack by a majority of the groups will succeed. Suppose further that the groups are dispersed, meaning that the general for each group must send messages between the various groups to relay the time to attack. Complicating matters, some generals may not obey instructions, and some might actually seek to sabotage the attack, conveying incorrect timing information to others. How can the participants be assured of a coordinated attack?

In the context of modern Blockchains, there is no way to proceed safely unless all participants in the network agree on things (such as whether they are all going to recognize a transaction as valid) absent a solution to the Byzantine Generals Problem. Certainly in a decentralized, massive network, trust would not work. A middleman would require some payment for coordinating a transaction and, in addition, this introduces the

---

cryptographic code." Alyssa Hertig, *How Do Ethereum Smart Contracts Work?*, COINDESK, https://perma.cc/JX2K-F6SX.

81. If a more detailed and involved explanation is desired, see *Basic Primer, supra* note 56.

82. By way of illustration, one of the requirements in order to become a licensed Virtual-Currency Business under the recently promulgated Uniform Act is that the business must file an application which demonstrates it has "policies and procedures for . . . an informational and operational security program . . . ." UNIF. ACT, *supra* note 13. Section 202 makes it unlawful for a virtual-currency business to operate without a license; Section 202(a)(2)(U) requires an application for a license to demonstrate requirements with article 6, which lists mandated compliance programs; and Section 601(a)(1) requires these programs. *Id.*

83. Alex Moskov, *What is the Byzantine Generals Problem?*, COINCENTRAL (Apr. 11, 2018), https://perma.cc/D8WZ-SKXK.

risk that the middleman could be compromised by an outside source or hack.

Bitcoin, thanks to the innovations by the person(s) known as Satoshi Nakamoto, was able to solve this problem by inventing something now known as the Proof-of-Work Protocol (sometimes called PoW). This protocol works as follows: a transaction is reported to the network. At that point every network Node (i.e., every computer with access to the network) examines the ledger to ensure the transaction is legitimate (i.e., does the ledger show that the transferor has the Bitcoins that are proposed to be transferred). Once the transaction is accepted as legitimate, it becomes part of the aggregated transactions that form a potential Block in the chain. However, in order to actually be added to the chain, the Nodes must solve a mathematical puzzle or problem which is known as the "Proof-of-Work."[84] Nodes that attempt to solve the puzzle are said to be Miners, and a Miner that successfully solves the puzzle sends the solution to the network for verification.[85] Upon verification, that Block becomes part of the Chain, and the Miner is rewarded for the "work" in solving the puzzle.[86]

The Proof-of-Work mechanism successfully solved the Byzantine General's Problem, but unfortunately there are some issues with it as a consensus protocol. First and foremost, Proof-of-Work is an extremely inefficient process because of the sheer amount of power and energy that it consumes.[87] Moreover, given that Cryptocurrencies were often lauded for their democratic character, the fact that wealthier people and organizations who can afford faster and more powerful Application-Specific Integrated Circuit (ASIC) devices have a better chance of Mining than others has been viewed as incompatible with the goals behind the technology.[88]

In response to these concerns, several Cryptocurrency projects have been working on alternatives to Proof-of-Work. The first of the

84. Debraj Ghosh, *How the Byzantine General Sacked the Castle: A Look Into Blockchain*, MEDIUM (Apr. 5, 2016) https://perma.cc/WLR7-GEAU.

85. *Id.*

86. *Id.*

87. Mining of Bitcoins in particular has become so widespread in certain areas that the amount of energy required for these operations has been in the news. Cyrus Farivar, *In Iceland, Bitcoin Mining Will Soon Use More Energy than Its Residents*, ARS TECHNICA (Feb. 12, 2018, 3:19 PM), https://perma.cc/P6NS-ZARM. The negative impact of these operations on the environment has received considerable attention in the news. Bloomberg, *Bitcoin Has a Dirty, Dirty Secret*, FORTUNE (Dec. 15, 2017), https://perma.cc/A8KH-6DM8.

88. Christoph Bergmann, *Bitcoin Subverts Power, But this does not make it Democratic*, BTCMANAGER.COM (Feb. 11, 2017, 8:19 PM), https://perma.cc/C3A4-H9BE. For a consideration of which ASIC devices are best for Bitcoin Mining, see Nate Drake, *Best ASIC Devices for Bitcoin Mining in 2018*, TECHRADAR (July 11, 2018), https://perma.cc/L46R-9SZT.

alternatives involves Proof-of-Stake (PoS) Protocols.[89] The idea behind this approach is simple: the more you invest in the coin, the more you gain by Mining with this protocol.[90] Proof-of-Stake requires a functional consensus distribution algorithm that rewards earnings based on the number of Coins a Node owns or holds (or other attributes such as age or duration).[91] The environmental reason for this shift is readily apparent; instead of thousands of computers Mining simultaneously, all you need is one computer with all of a user's holdings on it. Reportedly, the first Cryptocurrency to adopt the Proof-of-Stake method was Peercoin.[92]

Cardano, a fully open-source, decentralized public Blockchain project, is developing a Smart Contract Proof-of-Stake platform based on its Ouroboros algorithm.[93] Because of its innovative work in this area, it has been described as a leader in this space.[94] The Cardano project explains its commitment to the Ouroboros algorithm as being based on concern for the extreme environmental impact of Proof-of-Work Protocols.[95]

Ethereum[96] is also planning to move from Proof-of-Work to Proof-of-Stake, under a process that is somewhat different from that

89. For a relatively basic description of Proof of Stake, see *Proof of Stake (PoS)*, INVESTOPEDIA, https://perma.cc/2572-TSXS.

90. *Id.*

91. *Id.*

92. Amy Castor, *A (Short) Guide to Blockchain Consensus Protocols*, COINDESK (Mar. 4, 2017, 11:50 AM), https://perma.cc/5ZJK-LSZ9 (noting that the next two Cryptocurrencies to move to Proof-of-Stake were blackcoin and NXT).

93. cryptotoid, *Proof of Stake—Is it the Future?*, STEEMIT BETA, https://perma.cc/B5YH-SMJP. The Cardano project was started by IOHK, a technology company founded by Charles Hoskinson and Jeremy Wood, two of the co-founders of Ethereum. Michael Parsons, *Cardano: A Blockchain with Privacy and Regulation*, MEDIUM (Apr. 18, 2017), https://perma.cc/DN68-EWH6.

94. *See* Parsons, *supra* note 93.

95. One source states that

> Running the bitcoin protocol is a very expensive endeavor which uses large amounts of energy. It is estimated that 3.8 American households can be powered for a day by the energy that is spent to generate one bitcoin transaction. These energy requirements for running the bitcoin protocol continue to grow as more and more bitcoin miners sink money into mining. In addition, more energy is needed as the difficulty of the problems that their computers or mining rigs, encounter increases.

Ouroboros Proof of Stake Algorithm, CARDANO, https://perma.cc/K467-ZKKU.

96. While "Ethereum" is often used to refer both to the platform and the Token which powers the platform (*see infra* Section II.12.3), in this context it is the platform that is being discussed. Ethereum is actually a decentralized, open-source platform created by the Ethereum Foundation, described on the Ethereum website as "a Swiss non-profit, with contributions from great minds across the globe." *See* ETHEREUM, https://perma.cc/SXP7-DNX6. The power of this network is demonstrated by the fact that its Token, Ether, has the

proposed by Cardano. The Ethereum project is working on a network upgrade known as Casper, which will allow users to "stake" their Ether Tokens.[97] Validators, who must own enough Ether to be eligible to participate, will lock up some of their Ether in order to support bets.[98] If they act maliciously, they lose their stake; those who act honestly will be rewarded with an interest proportional to the amount of Ether that they chose to stake.[99]

Other Blockchain Consensus Protocols have also been considered, including Proof-of-Activity, Proof-of-Burn, Proof-of-Capacity, and Proof-of-Elapsed-Time.[100] Currently, none of these seem to have gained widespread acceptance.[101]

8. Coins

Technically speaking, Coins are a form of Cryptocurrency that operate independently of other platforms.[102] Bitcoins and Altcoins (alternatives to

---

second largest market capitalization of any Cryptoasset, behind only Bitcoin. *See Top 100 Cryptocurrencies*, *supra* note 1. Along with Bitcoin, Ether has been recognized by the SEC as being so prevalent that it should no longer be looked at as a security under U.S. law. Louise Matsakis, *Rest Easy, Cryptocurrency Fans: Ether And Bitcoin Aren't Securities*, WIRED (June 14, 2018, 4:19 PM), https://perma.cc/CV9U-CD5N. The securities ramifications of Cryptocurrency transactions are briefly discussed *infra* Sections II.34, II.34.4, notes 414, 421–27, and accompanying text.

97. Lewis Gray, *Proof of Stake Is Coming, and Will Be a Game Changer*, CCN (Feb. 7, 2018, 7:05 PM), https://perma.cc/6QBT-X954.

98. *Id.*

99. *Id.* Ethereum has had developers working on the upgrade to Proof-of-Stake since 2014, and it has been live on the Ethereum testnet since January 2018 and currently requires at least 1500 Ether to participate. *Id.*

100. Castor, *supra* note 92. This article notes that, as of March 2017, the only Cryptocurrency using Proof-of-Activity was Decred, and the only one relying on Proof-of-Burn was Slimcoin (which was only partially active when that article was written). It also reported that the only Cryptocurrency working on Proof-of-Capacity was Burstcoin, and further reported that the problem with Proof-of-Elapsed-Time is that it requires trust in Intel, a potential problem that Blockchain was designed to resolve. It is also important to note that other ideas are likely to appear, and one or more of them may become popular over time. *Id.*

101. *Id.*

102. *Difference Between Cryptocurrency Coins and Tokens*, *supra* note 40. Bitcoin, Dash, and Litecoin are identified as examples of Coins. *Id.* Coins, in most functional respects, operate like Tokens. The explanation of Tokens contained in this article is therefore also relevant to an understanding of Coins. *See infra* Section II.34. Coins can also can be divided into additional categories, beyond "Bitcoin" and its traditional alternatives. For example, Meta Coins add additional features designed to increase functionality of the coin, while coins can be said to be "coloured" if they have certain attributes. Those details may be more specific than this article needs, but if more information is sought, see Antonio

Bitcoins) are examples of this kind of cryptoasset.[103] Coins are also sometimes called crypto-coins.[104]

9. Coinbase

Coinbase is a digital trading platform founded in June of 2012, headquartered in San Francisco, California.[105] It claims 20 million or more users with more than $150 billion traded.[106] Coinbase has been described as "one of the most popular and well-known brokers and trading platforms in the world."[107] The goal of the platform is to make it easy to securely buy, use, store, and trade Digital Currency.[108] The company allows purchases of certain Cryptocurrencies (which vary depending on the country in which the trader is located) through a digital Wallet or through trading on the company's Global Digital Asset Exchange (GDAX) subsidiary.[109] GDAX operates in a number of countries, including the U.S., and has been praised as having a "[g]ood reputation, security, reasonable fees, [being] beginner friendly, [and having] stored currency [that] is covered by Coinbase insurance."[110] On the other hand, it has also been described as lacking adequate customer support, and having "limited payment methods, limited countries supported, [and] non-uniform rollout

---

Madeira, *What are Coloured Coins and Meta Coins?*, CRYPTOCOMPARE (July 30, 2018), https://perma.cc/ZN7M-KRWT, and Peter Van Valkenburgh, *What are Forks, Alt-coins, Meta-coins, and Sidechains?*, COINCENTER (Dec. 8, 2015), https://perma.cc/JWK6-8HY8.

103. Bitcoin was the original Cryptocurrency and is the one that most people have heard the most about. Coins that were specifically designed as "alternatives" to Bitcoin have come to be called "Altcoins." *See supra* Sections II.2–II.3 for a description of Altcoins and Bitcoin, respectively.

104. There are actually a number of words that have been used to describe essentially the same thing. "Cryptocoins, also called cryptocurrency or crypto, are a form of digital currency powered by blockchain technology. Cryptocoins do not have a physical, real-world equivalent.... Cryptocoins are purely digital." Brad Stephenson, *What are Cryptocoins?*, LIFEWIRE, https://perma.cc/TM72-8HNE.

105. *About Coinbase*, COINBASE, https://perma.cc/M999-7VGM.

106. *Id.*

107. *Best Cryptocurrency Exchanges: The Ultimate Guide*, BLOCKGEEKS (2018), https://perma.cc/F2LD-ERBA.

108. The Coinbase official website claims that it "is the easiest [and most trusted] place to buy, sell, and manage your digital currency." COINBASE, https://perma.cc/4L6Y-J4TJ.

109. GDAX is a regulated Bitcoin exchange with backing from the New York Stock Exchange, various banks, and venture capitalists. Greg Bensinger, *First U.S. Bitcoin Exchange Set to Open*, WALL ST. J. (Jan. 28, 2015), https://perma.cc/4TBQ-JZVN. The GDAX homepage explains that "GDAX offers institutions and professionals the ability to trade a variety of digital currencies like Bitcoin, Ethereum, and more on a regulated U.S. based exchange." *GDAX*, BITCOIN WIKI, https://perma.cc/T7XN-VDRD.

110. *Best Cryptocurrency Exchanges*, *supra* note 107.

of services worldwide," with the conclusion by some that "GDAX [is] suitable for technical traders only."[111] In early 2018, its base cost was a 4% fee on U.S. based transactions, although the exact amount charged varied "depending on whether you're using a bank account, a credit/debit card or a digital Coinbase wallet full of U.S. Dollars."[112]

10. Coincheck

Coincheck is a Tokyo-based Exchange or trading platform that promoted itself as having the number one Bitcoin trading volume in Japan.[113] In early 2018, it was hacked, infamously losing $530 million in NEM Tokens.[114] Coincheck froze transactions on its platform following the hack. As of August 15, 2018, the official Coincheck site still stated that "[c]urrently, we have suspended various features on our platform including new registrations."[115] Coincheck is only one of a number of digital currency trading platforms, but this experience should serve as a cautionary warning about some of the risks associated with trading on platforms based outside of the U.S. Of course, regulation in the U.S. is also lagging behind technological developments, and there are no widely accepted standards by which such trading platforms are evaluated or rated.[116]

111. *Id.*

112. Jacob Kleinman, *Consider These Digital Currency Exchange Alternatives to Coinbase*, LIFEHACKER (Jan. 5, 2018, 9:45 AM), https://perma.cc/F5MU-GWVT.

113. COINCHECK, https://perma.cc/3SEJ-ALYR.

114. Taylor Hatmaker, *Coincheck Users Are Suing To Get Their Money Off The Hacked Cryptocurrency Exchange,* TECHCRUNCH, (Feb. 12, 2018), https://perma.cc/7MB9-KDDA. NEM Tokens are still available. For a description of NEM, see *The Smart Asset Blockchain*, NEM, https://perma.cc/78F7-4VZN.

115. COINCHECK, *supra* note 113. Since the site has kept the same disclaimer for more than six months, the future viability of the service is in doubt, although the page does claim that the service is doing its "utmost to resume normal operations as soon as possible." *Id.*

116. Stock exchanges in the U.S., for example, have long been regulated by the SEC under section 6 of the Securities Exchange Act of 1934. 15 U.S.C. § 78(f). According to the SEC, exchanges offering trading in tokens have been reluctant to comply with the typical regulatory requirements, and the SEC has been "underwhelmed" by efforts of such exchanges to adhere to regulations applicable to stocks. *See* William Suberg, *SEC: US Crypto Exchanges Not 'Enthusiastic' Enough About Regulatory Compliance*, COINTELEGRAPH (June 7, 2018), https://perma.cc/2RLJ-KCVU. This leaves investors with little guidance in how to evaluate the reliability of most crypto exchanges. *Cf. supra* note 109, discussing GDAX.

11. CoinDesk

CoinDesk is a news site focusing on Blockchain technology and digital currencies.[117] It describes itself as "the leading digital media, events and information services company for the crypto asset and Blockchain technology community. Its mandate is to inform, educate and connect the global community as the authoritative daily news provider dedicated to chronicling the space."[118] It claims to have more than 5 million unique visitors with 50 million hits each month.[119]

12. Cryptocurrency

"Cryptocurrency" is a term that is not always used to mean precisely the same thing. Sometimes it is used for both Coins and Tokens, regardless of how they are intended to function. One source, for example, says that "Cryptocurrency" is generally understood as covering the realm of exchangeable value Coins and Tokens.[120] Coinmarketcap, a website that tracks Cryptocurrency capitalization, divides Cryptocurrencies into Coins and Tokens,[121] with the platforms utilized by each listed Token also being included.[122] Some sources disagree with this taxonomy and instead limit "Cryptocurrency" to the world of Coins, using the term "Cryptotoken" to refer to Tokens.[123] Tokens can have functions other than serving as a substitute for Fiat currency which is why some commentators object to them being classified as Cryptocurrencies.[124]

---

117. COINDESK, https://perma.cc/V6TL-E4V8.

118. *Id.*

119. *Id.*

120. *See* Aziz, *Coins, Tokens & Altcoins: What's the Difference?*, MASTERTHECRYPTO, https://perma.cc/695F-E6WT ("[A]ll coins and tokens are regarded as cryptocurrencies, even if most of the coins do not function as a currency or medium of exchange."); *see also* P.H. Madore, *What Is a Token In Cryptocurrency*, CRYPTOBRIEFING (June 19, 2018), https://perma.cc/3EFU-GTE2 (referring to all Cryptocurrencies, including Bitcoin, as Tokens).

121. *Top 100 Cryptocurrencies*, *supra* note 1.

122. *Id.* All but one of the top 10 Tokens in terms of market capitalization are hosted on Ethereum, while Tether (number 4 as of May 2018, with a market capitalization of $212 billion) is hosted on Omni. *Id.*

123. *See, e.g.*, Aziz, *supra* note 120, suggesting that "Cryptocurrency" is a misnomer, since many Coins and Tokens that followed Bitcoin do not possess the traditional characteristics of currency such as being a unit of account, a store of value, and a medium of exchange; *see also infra* Section II.34 for an expanded discussion regarding Tokens.

124. For a consideration of the possible functions of Tokens other than as a currency substitute, see *supra* note 38, *infra* Section II.34, and especially *infra* notes 318–25 and accompanying text.

There is no consensus on whether any particular usage is more correct. Instead, it is important to realize that clients may be speaking of Coins alone or both Coins and Tokens when they refer to "Cryptocurrencies." In fact, this lack of precision in terminology is one of the many factors that makes basic research into this emerging field so difficult. Since various sources discussing concepts relevant to Cryptocurrencies are inconsistent in their use of the technical terms, care must be taken in trying to understand the context in which particular comments are made.

The following examples focus on a few of the more important Cryptocurrencies (both Coins and Tokens) that are currently in existence. Some of these were designed to function as alternatives to Fiat currency,[125] and some have other functions that may be even more important to purchasers.[126]

12.1 Example—Bitcoin

Bitcoin[127] was the first widely accepted and successful Cryptocurrency built on a decentralized peer-to-peer network, and it has become the de facto standard for Cryptocurrencies.[128] The currencies inspired by Bitcoin are collectively called Altcoins and have generally tried to present themselves as modified or improved versions of Bitcoin.[129] While some of these currencies are easier to Mine than Bitcoin,[130] there are tradeoffs, including greater risk brought on by lesser liquidity, acceptance, and value retention.[131]

In techno-speak, Bitcoin utilizes Distributed Ledger Technology,[132] relying on Cryptographic Hashing which allows traders to use a system of

125. *See infra* Section II.21 for discussion of Fiat Currency.

126. For an additional explanation of the difference between Cryptocurrencies intended to act as replacements for traditional currencies and those with other utility, see Josiah Wilmoth, *The Difference Between Utility Tokens and Equity Tokens*, STRATEGIC COIN, https://perma.cc/4Y2G-HR4X.

127. *See supra* Section II.3 for more detail on Bitcoin.

128. Prableen Bajpai, *The 6 Most Important Cryptocurrencies Other Than Bitcoin*, INVESTOPEDIA (June 22, 2018, 3:08 PM), https://perma.cc/4WKP-C8KY.

129. The official websites for many of the alternatives often contain these favorable comparisons. *See* LITECOIN, https://perma.cc/69MT-85CU (emphasizing its "instant, near-zero cost payments" with "faster transaction confirmation times and improved storage efficiency than the leading math-based currency."); *see also* MONERO, https://perma.cc/JV8U-KSLJ (emphasizing that Monero is fast and private so that users "can spend safely, knowing that others cannot see your balances or track your activity").

130. *See, e.g.*, the description of Litecoin, *infra* Section II.12.4.

131. Bajpai, *supra* note 128.

132. Distributed Ledger Technology is discussed *infra* Section II.18.

Public and Private Keys to safeguard their information and access to their digital assets.[133]

12.2 Example—Dash

Dash has been described as "a more secretive version of Bitcoin."[134] This product was originally launched in January of 2014 as "Darkcoin," but was rebranded in March of 2015 to become Dash (which stands for digital cash).[135] Dash is self-funded, meaning that when new Dash are minted, 10% are set aside to improve the functionality of the Cryptocurrency.[136] Another difference between Dash and Bitcoin is that Dash has a two-tiered structure involving "masternodes" that perform key functions such as determining which projects are funded and which private transactions are enabled.[137]

12.3 Example—Ether (also referred to as Ethereum)

Founded in 2013, Ether is a digital Token offered on the Ethereum network.[138] The terms Ether and Ethereum have come to be used interchangeably,[139] although speaking technically Ethereum is the Blockchain network or platform on which Ether operates. Ethereum was conceived to extend Blockchain use to areas beyond Virtual Currency applications and is designed to allow the use of Smart Contracts with decentralized functionality.[140] According to the Etherium website, "Ethereum is a decentralized platform that runs smart contracts:

133. Cryptographic Hash is defined *infra* Section II.13, and Public and Private Keys are discussed *infra* Section II.25.

134. From its outset, Dash emphasized privacy for its users. sajalali, *supra* note 53.

135. *Id.*

136. Jeff Kauflin, *Dash Is Up 8,000% In 2017. Is This 'Darkcoin' A Better Version Of Bitcoin?*, FORBES (Dec. 22, 2017), https://perma.cc/HWL9-9WS8.

137. *Id.* "To become a masternode, you must buy at least 1,000 dash coins .... When new coins are created, 45% of them go to miners, 45% go to masternodes, and 10% go to the network." *Id.* When that story was written, the buy-in was approximately $1 million. *Id.* As of February 15, 2017, the buy-in would have been approximately $700,000. *Top 100 Cyrptocurrencies*, *supra* note 1. As of May 11, 2018, the buy-in would have been about $392,000. *Id.* By August 15, 2018, the price would have dropped to about $156,000. *Id.*

138. Ethereum has highlighted the ability of its platform to support smart contracts. Julia Beyers, *5 Of The Most Innovative Cryptocurrencies To Watch*, CRYPTOCOIN.NEWS (Jan. 16, 2018), https://perma.cc/Y3BX-ENJT.

139. One commentator described this "casual interchangeability" as a "common headache." Frederick Reese, *Ether vs. Ethereum: What Is the Difference?*, BITCOIN MARKET J. (Dec. 26, 2017), https://perma.cc/E5T4-3P88.

140. *Id.* Thus, the Ethereum platform allows moving and storing value on the web or in applications, creating completely new economic models for applications.

applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference."[141] Ether is the platform-specific Token that facilitates the development and functioning of such applications. In other words, "Ether is like a vehicle for moving around on the Ethereum platform" [142] and is sought by developers looking to "create markets, store registries of debts or promises, move funds . . . and many other things . . . without a middleman or counterparty risk."[143]

As was the case with Bitcoin, given the volume of fiat involved, it is not surprising that hackers were very interested in exploiting vulnerabilities in the system. While the Ethereum platform has never been compromised, in 2016 there was an attack on an Ethereum-based project known as The DAO[144] where 3.6 million Ether was hacked.[145] As a consequence, Ethereum was split via a Hard Fork into Ethereum (ETH) and Ethereum Classic (ETC).[146] It is the newer Ethereum (ETH) which has achieved such success, although ETC is also still trading.[147] In fact, based on current market capitalization, Ethereum is the most popular alternative to Bitcoin.[148] On the other hand, some commentators would characterize Etherium as something other than a "Cryptocurrency," since it was not conceived as a "currency," does not truly act as such despite the fact that it

141. ETHEREUM, https://perma.cc/SXP7-DNX6.

142. Bajpai, *supra* note 128.

143. ETHEREUM, *supra* note 141.

144. While DAO generally refers to Decentralized Autonomous Organization, as described *infra* Section II.14, "The DAO" was a specific DAO programmed and launched on April 30, 2016. David Siegel, *Understanding The DAO Attack*, COINDESK (June 25, 2016), https://perma.cc/U7HL-4UUF. The DAO offering attracted approximately $150 million worth of Ether in exchange for DAO tokens, which it was then going to use as a kind of venture capital fund for decentralized cryptocurrency projects. Emma Avon, *The DAO Hack–What Happened and What Followed?*, COINCODEX, https://perma.cc/KLY4-LV6U.

145. The drained Ether has not been accessed, but its sudden removal from the system triggered a rapid drop in the value of Ether from over $20 to under $13. Siegel, *supra* note 144.

146. Bajpai, *supra* note 128.

147. *See, e.g.*, *Top 100 Cryptocurrencies*, *supra* note 1 (listing ETC with a market capitalization of $3.28 billion as of February 18, 2018).

148. As of February 18, 2018, the total market capitalization of Bitcoin was over $182 billion, while Ethereum claimed a market capitalization of more than $92 billion. *Id.* Ripple's XRP Token was third on the list with about $44 billion in capitalization. *Id.* Several months later, in May of 2018, the top three Cryptocurrencies were still Bitcoin (total capitalization of $145 billion), Ethereum (total capitalization of $67 billion), and Ripple (total capitalization of $26 billion). *Id.*

is widely traded by speculators, and does not have a restricted supply.[149] Regardless of how it is characterized, it is by far the favored hosting platform for Tokens.[150]

12.4 Example—Litecoin (LTC)

Litecoin was introduced in 2011, with the stated objective of becoming the "silver" to Bitcoin's "gold."[151] As of May 11, 2018, Litecoin's market capitalization was approximately $7.85 billion.[152] While it falls considerably below Bitcoin's capitalization of approximately $145 billion, it is certainly not an insignificant amount. There are certain attributes that distinguish Litecoin from Bitcoin. One difference, which may be more apparent than real, is that Bitcoin is limited to 21 million Coins, while Litecoin can issue up to 84 million Coins.[153] This is not likely to have any practical significance because both Coins can be divided into extremely small fractional amounts.[154] A potentially more significant difference is the speed with which transactions are confirmed. While transactions themselves occur instantaneously, it takes an average of ten minutes for the Bitcoin network to confirm transactions, while the equivalent figure for Litecoin is approximately two-and-a-half minutes.[155]

149. *See generally* Frank Etto, *Know Your Coins: Public vs. Private Cryptocurrencies*, NASDAQ (Sept. 22, 2017) (on file with the Campbell Law Review).

150. As of May 2018, only three of the fifty Tokens with the highest market capitalizations relied on a platform other than Ethereum (with one being hosted on Omni and two on NEO). *Top 100 Cryptocurrencies*, *supra* note 1.

151. Litecoin is used for peer-to-peer payments. *What is the Difference Between Litecoin and Bitcoin?*, COINDESK, https://perma.cc/UT3F-4STE (last updated Apr. 2, 2014).

152. *Top 100 Cryptocurrencies*, *supra* note 1. This is a decrease from the approximate capitalization of $8.7 billion in February 2018. *Id.*

153. Jason Fernando, *Bitcoin vs. Litecoin: What's the Difference?*, INVESTOPEDIA (Feb. 15, 2018, 3:38 PM), https://perma.cc/84K4-PRRF.

154. *Id.* (noting that "the minimum quantity of transferable bitcoin is one hundred millionth of a bitcoin (0.00000001 bitcoins) known colloquially as one 'satoshi.'").

155. The ten minute Mining time for Bitcoin is explained in *Why Do Bitcoin Transactions Take 10 Minutes?*, BEST BITCOIN CASINOS, https://perma.cc/32E6-U83U (last visited December 10, 2018); *see also* Fernando, *supra* note 153 (discussing the Litecoin Mining speed). Note also that a Bitcoin transaction generally needs six confirmations from Miners before being processed, which would lead one to suspect that it would take a transaction about an hour on average to be added to the chain. However, the network has recently experienced considerable congestion. "The average time for one confirmation has recently ranged anywhere from 30 minutes to over 16 hours in extreme cases." Steven Buchko, *How Long do Bitcoin Transactions Take?*, COIN CENTRAL (Dec. 12, 2017), https://perma.cc/FMU3-TQ4U.

Litecoin also offers lower transaction fees than Bitcoin.[156] Perhaps the most significant difference between the two Coins involves the cryptographic algorithms which they each employ. Bitcoin utilizes the SHA-256 algorithm, while Litecoin makes use of a newer algorithm known as Scrypt, which affects how the Coins are Mined.[157] The SHA-256 algorithm is such that specialized hardware systems have become quite successful and overwhelmingly prevalent as Bitcoin Mining operations, while Scrypt "was deliberately designed to be less susceptible to the kinds of custom hardware solutions employed in ASIC-based mining."[158]

12.5 Example—Monero

"Founded in 2014, Monero is an open-source CryptoNote-based cryptocurrency that focuses on privacy."[159] Monero claims, on its website, that "[t]he most critical flaw in Bitcoin is its lack of privacy."[160] Given that belief, it is not surprising that Monero focuses on privacy as the attribute that distinguishes it from most other Cryptocurrencies. In fact, it has been reported that "Monero is favored for its untraceable and highly secure transactions."[161] Monero transactions are made anonymous by use of an integrated mixing process automatically applied to every transaction,[162] in contrast to the Bitcoin transactions, which are visible to the public once a Wallet address is provided.[163] Monero also claims a superior Mining algorithm, an "adaptive block size limit," and a particularly sophisticated development and research team.[164]

---

156. The price to send Litecoin is typically around $0.25, while the price to send Bitcoin ranges but is typically between $5.00–$25.00. *See Bitcoin, Litecoin Avg. Transaction Fee historical chart*, BITINFOCHARTS, https://perma.cc/HP23-L4V2 (last visited Sept. 28, 2018).

157. Fernando, *supra* note 153. For a brief explanation of Mining, *see infra* Section II.26.

158. Fernando, *supra* note 153.

159. Beyers, *supra* note 138. Monero offers money movement with an emphasis on privacy. *Id.* Monero has also been listed as one of the six most important Cryptocurrencies other than Bitcoin. *See* Bajpai, *supra* note 128. Monero's capitalization as of May 11, 2018 was approximately $3.2 billion. *Top 100 Cryptocurrencies*, *supra* note 1.

160. *The Merits of Monero: Why Monero vs Bitcoin*, MONERO.HOW, https://perma.cc/FCJ6-D2HB (last visited Dec. 10, 2018).

161. Beyers, *supra* note 138.

162. *See The Merits of Monero*, *supra* note 160.

163. Speaking technically, Ripple is the technology company behind the XRP Token, but common parlance often simply refers to the Token as "Ripple" notwithstanding the fact that Ripple has repeatedly explained that XRP is the name of an independent digital asset created but not owned by the company. Team Ripple, *The Difference Between Ripple and XRP*, RIPPLE (July 9, 2018), https://perma.cc/P8UR-U4Q3.

164. *The Merits of Monero*, *supra* note 160.

12.6 Example—Ripple (technically, Ripple's XRP Token)

Founded in 2012, Ripple (or more precisely its XRP Tokens)[165] was designed to facilitate fast, low-cost transactions between financial institutions.[166] In essence, it eliminates the limitations of conventional financial transactions caused when intermediaries are involved, particularly between unaffiliated banks.[167] Ripple is based on conventional SWIFT

165. Consider this statement from Coindesk, a self described crypto information service: "Ripple is the name for both a digital currency (XRP) and an open payment network within which that currency is transferred." Ariella Brown, *10 things you need to know about Ripple*, COINDESK (May 17, 2013, 11:00 AM), https://perma.cc/F6RN-SLHD. Another source explains that "[t]he first thing to know is that Ripple is both a platform and a currency." *What is Ripple. Everything You Need to Know*, COINTELEGRAPH, https://perma.cc/E9QH-9A9E (last visited Dec. 10, 2018). A simple google search on whether investment in Ripple is a good idea pulls up a plethora of articles, reinforcing the notion that many people simply say Ripple when they really mean the XRP Token.

There has been so much confusion about the distinction between Ripple and XRP that the Ripple team has created a chart to illustrate the differences. *See* Team Ripple, *supra* note 163. In essence, Ripple is the underlying company and XRP is an independent digital asset used to access certain Ripple services. *Id.*

166. For example, suppose Bank A, a Swiss Bank, needs to accept a payment in foreign currency from an unaffiliated Bank, and then transmit the payment to another unaffiliated Bank in a third country and in another currency. The delays and expense associated with converting currencies could be avoided by conducting exchanges with Ripple's XRP. "Rather than sourcing liquidity routes through numerous correspondent payment providers, thereby incurring numerous transaction costs, participants can cut out the middle men and transmit funds to one another directly." Joe Kendzicky, *Ripple (XRP) Analysis*, MEDIUM (May 4, 2018), https://perma.cc/MD74-W8J7.

The predecessor to Ripple, Ripplepay, dates back to 2004, before Bitcoin. *See* P4Man, *Ripple's XRP: Giving the Third-Largest Cryptocurrency a Second Look*, COINDESK (July 9, 2017), https://perma.cc/3DJ3-KGDW. Ripplepay was a peer-to-peer payment network, and it was acquired by OpenCoin which later became Ripple. *Id.* XRP Tokens are essentially designed to facilitate money movement for banks and other financial institutions. "Ripple created XRP tokens to seamlessly pay transaction fees between financial institutions, allowing funds to be promptly transferred between banks that have agreed to use this service. A transaction can happen at astonishing speed—in a few seconds." Mark Kaufman, *What the heck is Ripple? A brief look at the hottest cryptocurrency of the moment*, MASHABLE (Dec 29, 2017), https://perma.cc/98DF-KGAX. Ripple has indicated that its plans ultimately call for creation of about 100 billion Ripples, half of which would be retained by the company. Brown, *supra* note 165.

167. Beyers, *supra* note 138. One source listed Ripple as one of six most important Cryptocurrencies other than Bitcoin. *See* Bajpai, *supra* note 128. Note that the XRP Token is technically distinct from Ripple, the company, although common usage often conflates the two terms. Ripple has other viable Tokens in addition to XRP. *See* Andrew McElroy, *Ripple Tokens Could Be Worthless*, SEEKING ALPHA (Jan. 16, 2018, 9:57 AM), https://perma.cc/7AYT-LD4E.

banking principles and currently works with more than 100 banks.[168] By the end of February 2018, the market capitalization of Ripple approached $50 billion, although, by May 2018 this had declined to just over $26 billion.[169]

Despite its rapid recent rise in value, Ripple has been criticized as lacking many of the fundamental characteristics that are the traditional hallmarks of Cryptocurrencies.[170] The XRP Token was not designed to function as a currency, and Ripple chose to focus solely on strengthening the underlying Blockchain rather than giving any priority to supporting the value of the XRP Token.[171] There are other characteristics that distinguish Ripple's XRP from conventional Cryptocurrencies. For one, XRP has no Miners[172] and relies on a "centralized" Blockchain for speed and security.[173] Its Blockchain is not open, and although information is safely stored and protected through cryptography, only "trusted" operators in the network are allowed access.[174] Even the founders of Ripple recommend against using XRP as currency or an investment, but given the surge in trading value during 2017, clearly not everyone agrees.[175]

Despite concerns by some that XRP is not a "true" Cryptocurrency, it is included here because it has some serious financial weight behind it,[176] and it is at least now listed as a trading option on a number of Exchanges.[177] From a legal perspective, Ripple's XRP is most likely to be important to Banking clients because of its functionality.[178]

---

168. McElroy, *supra* note 167.

169. The total capitalization for Ripple's XRP on February 13 was $39,989,127,340. *Top 100 Cryptocurrencies*, *supra* note 1. On May 11 it was $26,027,058,043. *Id.*

170. Joe Liebkind, *Why Some Claim Ripple Isn't a 'Real' Cryptocurrency*, INVESTOPEDIA (Dec. 14, 2017, 1:55 PM), https://perma.cc/YE5Y-GWJ2.

171. *Id.*

172. *Id.*

173. Robert Greenfield, IV, *Ripple (XRP) is for the Banks, Not You*, MEDIUM (June 20, 2017), https://perma.cc/3L88-G3ZN.

174. Liebkind, *supra* note 170.

175. *See Best Bitcoin Generator*, THELONIOUS (Jan. 23, 2018), https://perma.cc/9E7D-5PMB ("Many digital currency investors are hunting for the next big altcoin, hoping to find a new Bitcoin for the right price. And the best contender is Ripple."); *3 Reasons to Invest in Ripple*, WEALTHDAILY, https://perma.cc/6A8U-ARH8 (last visited Dec. 10, 2018) ("In 2017, Ripple's price surged over 3,733%.").

176. "In 2017, Ripple (XRP) recorded greater gains than Ethereum and Bitcoin. These gains have laid the foundation for Ripple to become fully established as a virtual currency to be used by major institutions." Jessica Whitley, *Ripple Could Hit $5 with Coinbase Listing*, CRYPTODAILY (Feb. 16, 2018), https://perma.cc/98PD-4S5N.

177. According to Ripple.com, as of May, 2018, Ripple could be purchased on Bitstamp, Kraken, Coinone, Bitso, Coincheck, Korbit, Qryptos, Bitbank, Bitsane, M, LiteBit.eu,

12.7 Example—Zcash

Zcash is a decentralized and open-source Cryptocurrency launched in the latter part of 2016.[179] It describes itself like this: "If Bitcoin is like http for money, Zcash is https."[180] Zcash offers selective transparency of transactions so as to provide enhanced security.[181] Transactions are recorded and transmitted via the Blockchain, but details including the identity of the sender, the recipient, and the amounts involved are not published. [182] One source suggests that "Zcash's privacy strategy is essentially to erase the 'memory'—that is, the transaction history—of coins whenever a transaction occurs. . . . [B]y obfuscating transaction history, Zcash makes it impossible to trace transactions."[183]

13. Cryptographic Hash

The perceived immutable nature of a Blockchain ledger is rooted in the aggregation of time-stamped transactions into linear-sequenced Blocks. It is the aggregation into Blocks that permits the creation of links between transactions—the proverbial "chain" in the Blockchain. Each Block contains a unique Cryptographic Hash derived from the Block before it.[184] The function of the Cryptographic Hash is to authenticate the data in the

---

Bitcoin Co, Ltd., Gatehub, Bitcoin.co.id, Ces.io, and BitOasis. *XRP Buying Guide*, RIPPLE, https://perma.cc/L97Z-ZEEX (last visited Dec. 10, 2018).

178. Ripple was famously targeted by FinCen, the Financial Crimes Enforcement Network, a division of the Treasury Department, for "acting as a money services business" without registering its business, and for "failing to implement and maintain an adequate anti-money laundering (AML) program" to protect against access by money launderers or persons financing terrorist activities. Shane Ferro, *Regulators just demonstrated they are serious about making digital currency companies follow the rules*, BUSINESS INSIDER (May 5, 2015, 6:49 PM), https://perma.cc/CTK5-XUMF (quoting FinCen).

179. Zcash was designed to emphasize privacy. Bajpai, *supra* note 128. As of May 11, 2018, the total capitalization of Zcash was just under a billion dollars. *Top 100 Cryptocurrencies*, *supra* note 1.

180. ZCASH, https://perma.cc/38DZ-GY2D (last visited Dec. 10, 2018) ("If Bitcoin is like http for money, Zcash is https—a secure transport layer.").

181. *About Us*, ZCASH, https://perma.cc/L9HH-2W5M (last visited Dec. 10, 2018).

182. *Id.*

183. Etto, *supra* note 149. Zcash relies on an advanced cryptographic technique called zk-SNARKs to ensure privacy. *Id.*

184. A Cryptographic Hash "is a string of random-looking characters that uniquely identifies the data in question, much like your fingerprint identifies you. You can hash any data . . . by running the data through a hash generator. Every time you hash the same data, you will get the exact same hash value as a result." Bobby, *What is Cryptographic Hashing? MD5, SHA, and More*, TIPTOPSECURITY (Dec. 15, 2014), https://perma.cc/8RGX-A8Z5.

Block.[185] The resulting relationship between all the Blocks makes it virtually impossible to alter a prior entry in the digital ledger. This security feature is one of the most attractive attributes of Blockchain technology.[186]

14. Decentralized Autonomous Organization (DAO)

Not to be confused with "The DAO," which was a specific Decentralized Autonomous Organization,[187] a Decentralized Automonous Organization is a group that has done away with hierarchical management. Instead, it relies on Smart Contracts, or pre-programmed rules that describe how the system is to operate. The primary problem with this, and one which caused The DAO to fail after some months,[188] is that it is very difficult to change a DAO, or the Smart Contracts underpinning it, once the system is in operation. This can be a positive attribute, because no one person can unilaterally change the rules under which the system operates, but it is also a potentially huge disadvantage. If there is a problem, such as

---

185. Tim Fisher, *Cryptographic Hash Function*, LIFEWIRE (Aug. 7, 2018), https://perma.cc/7KBG-U2SP.

186. The attribute of immutability has been described as follows (all in the context of promoting Litecoin, a Token described in more detail *supra* Section II.12.4):

> Immutability, as it pertains to blockchains, is the idea that the public ledger can not be altered. This is an important trait for blockchains to have for several reasons:
>
> (1) The moment the rules of the protocol change for reasons outside of technical improvements, you open up pandora's box: Who's to determine what the criteria is for reversing transactions? Why does one situation fit but not another? Is there a difference between someone who had their coins stolen or sent to the wrong address? If not, how do they prove their LTC was stolen?
>
> (2) Without immutability, the blockchain itself is no longer a useful tool for verification because it's transactional history is subject to the community and/or developers. The reason for this is because those who break the rules will most likely break them again . . . .
>
> (3) It maintains fungibility. If a protocol were changed to suddenly "blacklist" LTC addresses because it is assumed they belonged to a thief, 1 LTC would no longer equal 1 LTC. 1 LTC would only equal 1 LTC as long as it's not associated with certain addresses.
>
> (4) It removes the "god-like" powers of developers. They are no longer able to determine the fate of the blockchain no matter what their intentions may be.

ECurrency Hodler, *The Importance of an Immutable Blockchain*, THE LITECOIN SCHOOL OF CRYPTO, https://perma.cc/XX3G-Q33J (last visited Dec. 10, 2018).

187. *See* Siegel, *supra* note 144.

188. Alyssa Hertig, *What is a DAO?*, COINDESK, https://perma.cc/KU5H-DZ4K (last visited Dec. 10, 2018).

a bug or exploitable weakness in the underlying code, developers cannot necessarily remedy the problem efficiently.[189]

15. Decentralized Applications (DApps)

Decentralized Applications (DApps) are a new sort of software,[190] intended to be more "flexible, transparent, distributed, [and] resilient" than traditional software models.[191] There is considerable agreement about what kinds of applications qualify as DApps.[192] For example, most sources agree that a DApp should be fully open-code, with adaptation to its protocol being decided by consensus of participants.[193] A DApp's data and operating reports must be encrypted and stored on a decentralized Blockchain.[194] A DApp must require a cryptographic Token (such as Bitcoin or an original application Token) for access to it.[195] Validation input contributed by Miners or others must be rewarded in DApp's Tokens.[196] In other words, a DApp is an application that is open source, operates autonomously, has its data stored on a Blockchain, is incentivised in the form of cryptographic Tokens, and operates on a protocol that shows Proof-of-Value.[197]

189. *Id.*

190. Traditional software apps usually owned or controlled by their creators or licensors, whereas DApps, by their nature, are decentralized. "Traditional apps build trust between users on the basis of past performance and business reputation. . . . [T]rust in Dapps is based on the technology itself . . . and doesn't require reputational or legal proofs." Michael Kordvani, *Dapp Development FAQs: How Different Are Dapps and Apps?*, B2B NEWS NETWORK (June 4, 2018), https://perma.cc/YD7C-R44R. This source suggests that "[t]he most exciting potential of Dapp development is in the creation of peer-to-peer marketplaces where users can complete transactions in a cheaper, safer, and faster way without the need for third parties that simply add more fees and longer, more cumbersome processes." *Id.* For a list of more than 1800 DApps hosted on Ethereum (a platform as well as a token, see supra Definition 12, Section 12.3), see *Explore Decentralized Applications*, STATE OF THE DAPPS, https://perma.cc/W4LW-TWPG (last visited Dec. 10, 2018).

191. Siraj Raval, *Chapter 1. What Is a Decentralized Application?*, O'REILLY, https://perma.cc/247V-AWQG (last visited Dec. 10, 2018).

192. *See* Alyoshkin, *supra* note 77.

193. *Id.; see also What Are Dapps? The New Decentralized Future*, BLOCKGEEKS, https://perma.cc/HT3M-N793 (last visited Dec. 10, 2018).

194. *What are Dapps?*, *supra* note 193.

195. Alyoshkin, *supra* note 77.

196. *What are Dapps?*, *supra* note 193.

197. Alyssa Hertig, *What is a Decentralized Application?*, COINDESK, https://perma.cc/NUX7-QCFA (last visited Dec. 10, 2018).

16. Digital Currency

Digital Currency generally refers to a non-physical (ie, electronic or digital) representation of traditional money or Fiat currency,[198] whereas a Virtual Currency[199] has no corresponding external value or existence.[200]

17. Digital Currency Exchange

An exchange of Digital Currency occurs when anyone uses online or digital resources (such as a credit or debit card, or an electronic check) to transfer Fiat Currency[201] to another person. This exchange may be regulated under traditional money transmitter laws, but those rules have been in place for some time with experts who understand how they apply.[202] On the other hand, when one buys a Virtual Currency[203] with Fiat, it may be very difficult to get the value back out in any useable form.[204] In order to accomplish this kind of exchange, a specialized exchange platform[205] may be required.

18. Distributed Ledger Technology

In the context of Blockchains, a "ledger" is simply a digital version of a database or spreadsheet that can store all sorts of information, which everyone can trust to be accurate. An online ledger maintained by Distributed Ledger Technology is decentralised because transactions are stored on up to several thousand computers connected to a common network via the internet.[206] Changes and updates to the ledger may only be made if the network of computers, relying on common software, reaches a consensus that the change or update is valid, which means that the ledger must incorporate a system-wide consensus protocol to maintain its

198. *See infra* Section II.21 for a discussion of Fiat Currency.

199. *See infra* Section II.36 for discussion of Virtual Currency.

200. Tara Annison, *Virtual vs Digital Currency—What's the Difference?*, MARKET MOGUL (July 22, 2017), https://perma.cc/M9FT-DYYN.

201. *See infra* Section II.21 for a discussion of Fiat Currency.

202. For an introduction to money transmission requirements see Marco Santori, *What is Money Transmission and Why Does it Matter?*, COINCENTER (Apr. 7, 2015), https://perma.cc/YH2S-V6WN.

203. *See infra* Section II.36 for a discussion of Virtual Currency.

204. Annison, *supra* note 200.

205. *See infra* Section II.20 for a discussion of Exchanges.

206. A very basic, non-technical explanation of Distributed Ledgers can be found at Shyam Shankar, *Centralized Ledgers Vs Distributed Ledgers (Layman Understanding)*, MEDIUM (July 12, 2017), https://perma.cc/AL3Q-VAWU.

integrity.[207] A Blockchain is therefore one type of distributed ledger; it is a decentralised peer-to-peer network of independent computers recording, sharing and synchronizing data according to preset protocols.[208] The Blocks of data stored on the Blockchain are in essence a ledger of accepted transactions.

Distributed Ledger Technology has particular significance in the financial sector, with the potential to make financial technology ("Fintech") more efficient, resilient, and reliable.[209] Fintech refers to companies and innovations that are designed to use technology in innovative ways to improve financial services. Experts predict particularly rapid changes in this sector of the world economy as a result on ongoing developments relating to Blockchain.[210]

19. Ethereum (the platform)

Ethereum is a "a decentralized software platform that enables Smart Contracts and Distributed Applications to be built and run without any downtime, fraud, control or interference from a third party."[211] "No one owns it. There are no venture investors backing Ethereum Inc., because there is no 'Ethereum, Inc.'"[212] Although there is no conventional business organization behind Ethereum, the team backing the project and encouraging innovation has been recognized for possessing an exceptional level of talent.[213] As a result, it is not surprising that as of May 11, 2018, Ethereum's primary Token, ETH (which is confusingly sometimes also called simply Ethereum), had a market capitalization exceeding $67 billion, placing it second only to Bitcoin.[214]

20. Exchanges

Cryptocurrency Exchanges are websites where Cryptocurrencies may be bought or sold, or exchanged for other Digital Currency or Fiat like U.S. dollars or Euro. Professional traders may seek out an Exchange such as

207. *Id.*; *see also supra* Section II.7 (describing various Blockchain Consensus Protocols).

208. *Blockchain & Distributed Ledger Technology (DLT)*, WORLD BANK (Apr. 12, 2018), https://perma.cc/2FVL-Q7BQ.

209. *Id.*

210. *Is distributed ledger technology (DLT) a banking fad or fixture?*, J.P. MORGAN, https://perma.cc/C7MK-FETN (last visited Dec. 10, 2018).

211. sajalali, *supra* note 53. *Accord* Beyers, *supra* note 138.

212. Steven Johnson, *Beyond the Bitcoin Bubble*, N.Y. TIMES (Jan. 16, 2018) (on file with Campbell Law Review).

213. Beyers, *supra* note 138.

214. *Top 100 Cryptocurrencies*, *supra* note 1.

Kraken or Bittrex.[215] Those kinds of Exchanges require participants to register, verify their identification, and have an account.[216] Occasional traders may rely on trading platforms that do not require an account although this is increasingly unusual.[217] Such platforms are websites that connect buyers and sellers and typically take a fee from each transaction. They may involve direct trading, where sellers set their own exchange rates, or may involve a broker who sets the exchange rate on the broker's website.[218] Exchanges are increasingly subject to regulatory requirements, and violation of applicable rules can result in substantial penalties being imposed.[219]

21. Fiat (or Fiat currency)

The concept of Fiat currency originally referred to something that had value as a medium of exchange, not because of any intrinsic or underlying value, but because people were willing to accept that it had value.[220] For

215. For a comparison of these two Exchanges, see Steven Buchko, *Kraken vs Bittrex Comparison*, COINCENTRAL (Oct. 2, 2017), https://perma.cc/V7TZ-S7L2. Bittrex is based in the US, and claims more the fifty years of experience in online security. *See* BITTREX, https://perma.cc/QK4A-4C9M. "Founded in 2011, Kraken supports a longer list of digital currencies that Coinbase, including Bitcoin, Ether, Monero, Augur REP tokens, ICONOMI, Zcash, Litecoin, Dogecoin, Ripple and Stellar/Lumens. It also supports a handful of traditional currencies, like the U.S. Dollar, Canadian Dollar, British Pound, Japanese Yen and the Euro." Kleinman, *supra* note 112. "Based in Slovenia, Bitstamp is one of the top exchanges when it comes to the number of trades processed. It supports Bitcoin, Ether, Litecoin, Ripple, and Bitcoin Cash, along with U.S. Dollars and Euros. Bitstamp is trusted and regulated, however, it can be tough to get used to if you're a beginner." *Id.*

216. Buchko, *supra* note 215.

217. One source suggests that the only time you would want a platform that does not require an account is if you "just want to make the occasional, straightforward trade." *Best Cryptocurrency Exchanges: The Ultimate Guide*, BLOCKGEEKS, https://perma.cc/F2LD-ERBA (last updates Sept. 13, 2018).

218. For a description of the various ways in which exchanges may operate, *see id.*

219. Obviously, the complexities of such regulation are far beyond the scope of this article. For a look at a couple of cases involving the potential for liability when a business improperly operate a Cryptocurrency Exchange, see United States v. Faiella, 39 F. Supp. 3d 544, 545 (S.D.N.Y. 2014) ("Defendants in this case are charged in connection with their operation of an underground market in the virtual currency 'Bitcoin' via the website 'Silk Road.'"); United States v. Lord, No. CR 15-00240-01/02, 2017 WL 1424806, at *2 (W.D. La. Apr. 20, 2017) ("Counts 2–14 charged Defendants with various other crimes associated with operating their bitcoin exchange business."). Notwithstanding the risk of liability, the SEC has been vocal in its criticism of how slow Cryptocurrency Exchanges have been to comply with regulatory requirements. *See* Suberg, *supra* note 116.

220. "Currency that is not backed by any type of physical asset or reserve is called fiat money. This term comes from the Latin and means something to the extent of 'as you wish.' The current fiat money system is essentially worldwide, since every country

the most part, in common usage, "Fiat" or "Fiat currency" refers to currency that is issued or backed by a governmental authority without being tied to any tangible asset (such as gold).[221] For example, American dollars have value as a medium of exchange first and foremost because the U.S. government has declared that they will be legal tender, and the public generally accepts that this is true.[222]

One of the driving theoretical underpinnings of Cryptocurrencies such as Bitcoin was that they offer comparative advantages over Fiat currencies, particularly in developing economies. Cryptocurrencies are not, for example, subject to hyperinflation because the supply of particular coins can be set as finite, preventing the problems that can occur when a government begins to print more and more cash.[223] It can avoid the problems of counterfeit currency.[224] Concerns over Fiat currency being rigged, coercive, favoring the wealthy, and leading to an increasingly unhealthy concentration of wealth have also been raised as reasons to prefer Cryptocurrencies.[225]

These concerns may lead some clients to being particularly committed to Cryptcurrency alternatives to Fiat currency, so at the very least it could be helpful to have an understanding of this mindset. Most experts, however, agree that it is likely that Fiat currency will continue to be essential to the functioning of developed economies.[226]

---

followed the path of the U.S. shortly after we went off the gold standard." Joseph Carducci, *The Problem With Fiat Currency—Will Fiat Currency Stick Around?*, OUTSIDER CLUB (June 13, 2013, 4:32 PM), https://perma.cc/47XE-EQZW.

221. *Fiat Money*, INVESTOPEDIA, https://perma.cc/QRA9-BL5M (last visited Dec. 10, 2018) (explaining that "Fiat money is currency that a government has declared to be legal tender, but it is not backed by a physical commodity.").

222. *See* Coinage Act of 1965, 31 U.S.C. § 5103 (2012) ("United States coins and currency (including Federal reserve notes and circulating notes of Federal reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues.").

223. For a discussion of this problem with existing Fiat Currency, see Oliver Dale, *The Problems with Fiat Currency*, BLOCKONOMI (Feb. 9, 2018), https://perma.cc/VB2R-QNS2 [hereinafter *Problems*].

224. For a discussion of this risk, see Tim Worstall, *Fiat Money Problems—Goodbye To The Round Pound And Welcome To The More Difficult To Forge One*, FORBES (Jan 1, 2017, 6:39 AM), https://perma.cc/9UYK-WSEL.

225. Ron Hera, *15 Fundamental Problems with Fiat Currencies*, FIN. SENSE (Mar. 26, 2012), https://perma.cc/VD4A-9XK5.

226. *See, e.g.*, Tim Swanson, *Why Bitcoin Needs Fiat (And This Won't Change in 2018)*, COINDESK (Jan. 3, 2018, 12:30 PM), https://perma.cc/3P9Y-XS53.

22. Forks (Hard and Soft Forks)

Forks create alternate versions of the Blockchain, leaving two Blockchains to run simultaneously on different parts of the network.[227] A Hard Fork renders some previously invalid transactions valid, and vice versa.[228] This type of Fork requires all Nodes and users to upgrade to the latest version of the protocol software.[229] A Soft Fork differs from a Hard Fork in that previously valid transactions are still valid, but the updated Nodes will no longer accept new transactions like the old ones.[230] Since old Nodes recognize the new Blocks as valid, a Soft Fork is essentially backward-compatible.[231] This type of Fork requires most Miners to upgrade in order to enforce, while a Hard Fork requires all Nodes to agree on the new version.[232]

23. Hardware Wallet

While a more complete definition of Wallets in general is found in Definition 37, a Hardware Wallet is a hardware device that stores the user's Private Keys, allowing the owner access to their Cryptocurrency accounts.[233] Although this does involve a tangible item (the "hardware"), it does not "hold" users' Cryptocurrencies, and instead is merely a vehicle for accessing their digital assets.[234]

24. Initial Coin Offering (ICO)

An ICO, or Initial Coin Offering, is the process by which issuers sell Cryptocoins or Tokens that they have developed in exchange for Fiat

227. *See* Amy Castor, *A Short Guide to Bitcoin Forks*, COINDESK (Mar. 27, 2017, 2:00 PM), https://perma.cc/4MQK-MF3H.

228. *Id.*

229. *Id.* (noting that in a Hard Fork, "all of the nodes in the network need to upgrade to the new rules").

230. *Id.*

231. *Id.*

232. For a description of the soft Fork considered by and the hard Fork taken by Ethereum in response to the hacking of The DAO, see *supra* notes 144–46 and *infra* notes 244–46 and accompanying text.

233. In somewhat more complicated but precise terms, "Cryptocurrency wallets are software programs that store your public and private keys and interface with various blockchain so users can monitor their balance, send money and conduct other operations." *Cryptocurrency Wallet Guide: A Step-By-Step Tutorial*, BLOCKGEEKS, https://perma.cc/AL6P-AK6F (last visited Dec. 10, 2018).

234. For a more detailed but non-technical explanation of Hardware Wallets in particular, see *Hardware Wallet*, BITCOIN WIKI, https://perma.cc/888V-4NGX (last updated Nov. 6, 2018).

Currency or other Virtual Currencies.[235] It has been compared to public offerings of securities in traditional Initial Public Offerings (IPOs).[236] Both IPOs and ICOs are often used to raise capital for a variety of business activities, but there are clearly major differences between the two. One practical difference is the nature of the underlying stake being acquired by the purchaser. In an IPO, shares generally represent ownership in the company that is raising funds,[237] whereas in an ICO the Coins or Tokens do not include direct ownership of the business.[238] In addition, the regulatory framework for the two options are radically different. IPOs are heavily regulated in most countries, whereas ICOs are still so new that they have been operating in the "gray" area while regulators are trying to develop and implement workable approaches to oversight.[239]

The first attempts at fundraising business ventures via the sale of Cryptotokens relied on relatively limited initial financing models. Ripple, for example, sold one billion of its XRP tokens in 2013 in exchange for about $5 million in Fiat currencies or Bitcoin.[240] In early 2014, Ethereum raised $18 million via an ICO, the largest completed ICO at that time.[241]

---

235. *What is an ICO?*, BITCOIN MAGAZINE, https://perma.cc/6Q7A-8ASB (last visited Dec. 10, 2018).

236. *Id.*

237. According to the SEC, an IPO (or initial public offering) occurs when a company goes public "by selling shares of stock to the public, usually to raise additional capital." *Going Public*, U.S. SEC. & EXCH. COMM'N, https://perma.cc/5L65-Q4J5 (last updated Nov. 28, 2017).

238. For an introductory overview of the ICO process, see *How To Buy ICO Tokens: Beginner's Guide*, COINTELEGRAPH, https://perma.cc/HY8S-KCKV (last visited Dec. 10, 2018). This source notes that once the tokens are acquired, they may be viewed as an investment, which may either be held or traded. The value of the token should go up as the company's value increases over time, and the tokens themselves may "provide investors with future access to the product or service as well as certain perks." *Id.* In neither case, however, does Token ownership equate to ownership or control over the issuer of the Token. *Id.*

239. Perhaps the most colorful observation about regulators' attempts to catch-up to the rapid developments in the crypto space was the observation that "fighting fraud in virtual currencies has almost become a game of Whack-A-Mole for regulators and federal prosecutors, who find each new iteration seemingly a few steps ahead them." Peter J. Henning, *Policing Cryptocurrencies Has Become a Game of Whack-a-Mole for Regulators*, N.Y. TIMES: DEALBOOK (May 31, 2018), https://perma.cc/V2FE-GB7Y.

240. *Id.*; *see also* George Alex Popescu, *Initial Coin Offerings (ICO)—New Funding Source?*, MEDIUM (July 26, 2017), https://perma.cc/24U8-2HLD. As of August, 2013, the sales price of these Tokens was around $.005, which would have allowed the Ripple ICO to raise about $5 million. For historical pricing information about Ripple, see *XRP Price Chart US Dollar (XRP/USD)*, COINGECKO, https://perma.cc/3Z9C-J6PP.

241. "The Ethereum ICO was a pioneer in the space of initial coin offerings and the team successfully raised $18 million in 42 days, making it the number one most funded ICO in

One of the largest early ICOs conducted on the Ethereum platform was both spectacularly successful and fatally flawed. The DAO[242] "promised to create a decentralized organization that would fund other blockchain projects, but it was unique in that governance decisions would be made by the token holders themselves."[243] The DAO ICO was successful in raising more than $150 million in a short amount of time,[244] but was unsuccessful in that the project included technical vulnerabilities that were exploited by a hacker who drained millions of dollars in value from the project before a "fix" could be agreed-upon and implemented.[245] As a result, Ethereum Foundation eventually decided to move forward with a Hard Fork, which allowed them to recover the stolen funds even though it split the community.[246]

Despite this rough start, the Ethereum platform has been remarkably successful at hosting ICOs.[247] For example, EOS recently raised approximately $700 million in its year-long ICO,[248] despite the fact that its FAQ page stated that "token-holders will not be afforded any rights or functions."[249] One site listing recent ICOs[250] lists both pending ICOs and

---

cryptocurrency." Emma Avon, *A timeline of the most successful ICOs*, COINCODEX, https://perma.cc/8BD6-897F (last visited Dec. 10, 2018).

242. For a brief introduction to The DAO and its hack, see *supra* notes 138–40 and accompanying text.

243. *What Is an ICO?*, *supra* note 235.

244. "The creation period was an unforeseen success as it managed to gather 12.7 Ether (worth around $150M at the time), making it the biggest crowdfund ever. At some point, when Ether was trading at $20, the total Ether from The DAO was worth over $250 million." Antonio Madeira, *The DAO, The Hack, The Soft Fork and The Hard Fork*, CRYPTOCOMPARE (July 26, 2016), https://perma.cc/6R49-Q42N.

245. About $70 million worth of Ether (in then-current value) was drained from The DAO within the first few hours of the hack. *Id.*

246. The community at first considered a Soft Fork that would have blacklisted transactions from the DAO, but this was ultimately determined not to be a viable solution. *Id.* Instead, the community split on the Hard Fork solution, which was designed to return the stolen Ether. Approximately 89% of Ether holders voted for this alternative and it occurred in July of 2016. *Id.*

247. Crowdfunding through ICOs has even been called Ethereum's "killer application" because of the successes of this process. *See, e.g.*, Joseph Young, *ICO Tokens: Ethereum's Killer App?*, CCN (June 7, 2017), https://perma.cc/L9HN-5CUE ("Based on the current trend of blockchain and the increasing demand for cryptoassets, it seems evident that Ethereum's killer app has been its infrastructure for ICO tokens."); Matthew Tan, *Ethereum's Killer App*, MEDIUM (Apr. 9, 2017), https://perma.cc/R37A-DVTS ("Ethereum's killers app are ICOs").

248. "EOS" is the proper name of the Token issued in that ICO. Samuel Haig, *EOS Raises $700M Despite Token Affording No "Rights, Uses, Purpose, or Features"*, BITCOIN.COM (Dec. 20, 2017), https://perma.cc/T5CG-3CYJ.

249. *Id.*

ICOs that have been completed within the past year. According to a late February, 2018 review of that site, the Tezos ICO had raised more than $230 million,[251] and the EOS ICO that ended July, 2017 raised nearly $197 million.[252] Other ICOs conducted between February 2017 and 2018 that raised more than $100 million each include: Qash (more than $106 million),[253] Filecoin ($257 million),[254] Status Network (more than $107 million),[255] Bancor ($153 million),[256] and MobileGo (more than $160 million).[257] While most of the ICOs listed on the site raised substantially less than $100 million, the total amount raised in ICOs ending in February 2018 alone exceeded $650 million.[258]

25. Key (Public and Private Keys or Key Pairs)

Transactions involving cryptographic Coins and Tokens need to be both authenticated and private. In other words, it is important that

250. ICODrops lists both current and completed ICOs. For a basic description of ICODrops, see *About,* ICODROPS (on file with Campbell Law Review). For a list of current or active ICOs, see *Active ICO,* ICODROPS (on file with Campbell Law Review). For a list of completed ICOs, *Ended ICO,* ICODROPS (on file with Campbell Law Review). For a list of upcoming ICOs, see *Upcoming ICO,* ICODROPS (on file with Campbell Law Review).

251. *Tezos,* ICODROPS (on file with Campbell Law Review).

252. *EOS,* ICODROPS (on file with Campbell Law Review). Contrast this with the $700 million claimed by Brock Pierce, chairman of the Bitcoin Foundation and advisor to as well as minority partner in EOS. Haig, *supra* note 248. Pierce reported that as of October, 2017 the EOS ICO had raised "almost" $700 million, claiming that the company was selling 2 million Tokens daily. *Id.* ("According to the Wall Street Journal, the figure is larger than that raised by 'all but 10 of the 195 U.S. initial public offerings this year.'").

253. *Qash,* ICODROPS (on file with Campbell Law Review).

254. *Filecoin,* ICODROPS (on file with Campbell Law Review).

255. *Status Network,* ICODROPS (on file with Campbell Law Review).

256. *Bancor,* ICODROPS (on file with Campbell Law Review).

257. *MobileGo,* ICODROPS (on file with Campbell Law Review).

258. This total was obtained by adding the amounts raised through ICOs listed by ICODrops as having been completed between February 1st and 20th of 2018. *Ended ICO, supra* note 250. On the other hand, by the end of February, 2018, some sources were reporting that more than half of the ICOs attempted in 2017 had already failed or were failing. Tom McKay, *Wow, Who Could Have Predicted 59 Percent of 2017's ICOs Are Already Dead or Doomed,* GIZMODO (Feb. 25, 2018, 2:45 PM), https://perma.cc/NU94-4QNL. Notwithstanding such pessimistic reports, the amounts being raised through ICOs continue to be significant. In March, 2018, for example, a single offering of "Dragon" (described as a "new digital currency, funded upon Ethereum Blockchain system and strongly underpinned by a substantial gaming business in Macau") raised $320 million. *Dragon,* ICODROPS, (on file with Campbell Law Review). In the first 10 days of May, a total of thirteen ICOs were concluded, raising more than $295 million. *Ended ICODrop, supra* note 250.

participants in a transaction involving the transfer of such interests be able to verify that the person with whom they are communicating (and to whom they are transferring assets) is the correct person, and to feel comfortable in knowing that unauthorized third parties will not have access to their private financial information. Public and Private Keys (two related, lengthy alphanumeric sequences) are part of the cryptographic system that accomplishes these two tasks.[259] A Public Key is made available to third parties (in a very rough sense like an email address that can be seen by anyone), while a Private Key is known only to its owner (again in very general terms, somewhat like a password).[260] The Private Key allows a user to generate a signature for each transaction authorized by the user with that signature being used to confirm the user's identity and the validity of the transaction.[261] The Private Key then uses a mathematical process to develop a Public Key, which is transformed via a Cryptographic Hash to produce the address that other people can see.[262] The nature of the cryptographic process is such that third parties cannot generally "reverse engineer" the hash so as to be able to decode the contents of the message, thus protecting the confidential nature of the information being transmitted.[263]

26. Mining (Miners)

Mining is the process by which transactions are verified and added to the public ledger, and in the case of Bitcoin and several other

259. *What is a Public and Private Key Pair?*, SSL2BUY, https://perma.cc/W9ZG-JVPE (last visited Dec. 10, 2018); *see also supra* Section II.31 (discussing "Signature").

260. The comparison between email addresses and passwords and Public and Private Keys is very rough indeed. Unlike paired Key cryptography, an email system does not prevent others (such as the email provider) from accessing the information, and does not allow verification of the sender's identity or authentication of the contents of the message. In addition, most people retain their email for more than a single message. In the context of cryptotransactions, users are often advised to change their address for every transaction in order to maximize confidentiality and security. *See supra* note 38 and *supra* Section II.1 (discussing "Addresses").

261. For a description of Public and Private Keys, and how they operate, see *Public Key and Private Keys*, COMODO, https://perma.cc/6HHR-6EQF (last visited Dec. 10, 2018).

262. For a further description of this process, see Leon Di, *Why Do I Need a Public and Private Key on the Blockchain?*, WE TRUST BLOG (Jan. 29, 2017), https://perma.cc/MBN7-WDX8.

263. Shaan Ray, *Cryptographic Hashing*, HACKERNOON (Nov. 3, 2017), https://perma.cc/EGW6-ZAP9. "Hashing is a mathematical operation that is easy to perform, but extremely difficult to reverse. (The difference between hashing and encryption is that encryption can be reversed, or decrypted, using a specific key.)." *Id.; see also supra* Section II.13 (discussing Cryptographic Hashing).

Cryptocurrencies, it is also the means through which new Coins are released. Anyone with access to the internet and suitable hardware can participate in Mining. The Mining process involves compiling recent transactions into Blocks and trying to solve a computationally difficult puzzle that appears at the end of each Block when it is added to the "chain."[264] The participant ("Miner") who first solves the puzzle gets to place the next Block on the Blockchain and claim the rewards.[265] The rewards, which may take the form of Coins or other agreed payment, incentivize Mining and act as the transaction fees associated with the transactions compiled in the Block. "Bitcoin Mining" is the process by which transactions in Bitcoin are verified and added to the ledger or chain. At the current time, the process results in the issuance of one new Bitcoin to the successful Miner for each Block verified.[266]

27. Multi-Sig (Multisignature)

In the context of Cryptocurrencies, Multi-Sig (or Multisignature) is a technology that adds another layer of security to the transaction verification process. Multi-Sig Addresses require multiple users to add their digital Signatures to a transaction before it can be broadcast to the network and added to the Blockchain.[267] This is not associated with every transaction, but can be used for increased security.[268]

28. Nodes

A Node refers to a computer connected to the Blockchain network using a client that performs the task of validating and relaying

264. Jordan Tuwiner, *What is Bitcoin Mining and How Does it Work*, BUY BITCOIN WORLDWIDE, https://perma.cc/266U-5WMY (last visited Dec. 10, 2018) (explaining that Bitcoin miners solve "a computational problem which allows them to chain together blocks of transactions.").

265. *Block (Bitcoin Block), supra* note 64. As a practical matter, because of the nature of the Proof-of-Work Protocols, and the algorithms used by Bitcoin, Mining for Bitcoin is only likely to be profitable after a specific investment in expensive ASIC equipment and then only in environments where energy and space are cheap and plentiful. *Id.* For a discussion of some alternative algorithms that may minimize these problems see *Posts Tagged 'low energy algorithms'*, CRYPTO MINING BLOG (July 8, 2014), https://perma.cc/7F6R-KXMF.

266. *See* Tuwiner, *supra* note 264.

267. For a more thorough but still basic description of Mulit-Sig, see Ariel Horwitz, *Multisig: A beginnerr's guide*, 99BITCOINS (Jan. 2, 2018), https://perma.cc/M2RQ-UQGZ.

268. For example, Wallets (*see infra* Section II.37) provide differing levels of security, and Multi-sig is offered in some to heighten protections against theft. *See generally* Redactor, *A Crypto-currency Wallet—What is it and Why You need a MultiSig Wallet?*, MEDIUM (Mar. 26, 2018), https://perma.cc/LNN4-T3XN.

transactions.[269] The computer gets a copy of the Blockchain, which is downloaded automatically when the computer joins the network.[270] Every Node becomes an "administrator" of the Blockchain upon joining, and in this sense, the network is decentralized.[271] Nodes may be full or lightweight, with a full Node having a copy of the entire Blockchain and therefore having the power to validate Blocks and transactions from other Nodes, while a lightweight Node essentially operates by trusting the full Nodes to perform the validation functions.[272]

29. Proof-of-Stake (PoS) and Proof-of-Work (PoW)

These are two different options for how consensus can be achieved in a decentralized, peer-to-peer network, and both are described in more detail as options in the definition of Blockchain Consensus Protocol.[273] PoW was the original protocol, utilized by Bitcoin and most of the initial coins that followed, while PoS is a more recent option designed to solve some of the problems that have arisen with PoW protocols.[274]

30. Simple Agreement for Future Tokens (SAFT)

SAFT stands for "Simple Agreement for Future Tokens," which is clearly a nod to the successful SAFE startup documentation project pioneered by Y Combinator.[275] In essence, this is a contract in which an

269. Technically speaking, Nodes "can be any active electronic device, including a computer, phone or even a printer, as long as it is connected to the internet and as such has an IP address." *Nodes*, LISK, https://perma.cc/5PXE-U6GX (last visited Dec. 10, 2018).

270. "The role of a node is to support the network by maintaining a copy of a blockchain and, in some cases, to process transactions." *Id.*

271. Tim Swanson, *Who are the administrators of blockchains?*, GREAT WALL OF NUMBERS (Oct. 19, 2017), https://perma.cc/MX86-VXUQ.

272. *See* Bisade Asolo, *Full Node and Lightweight Node*, MYCRYPTOPEDIA (Nov. 1, 2018), https://perma.cc/EX4T-XG3N. Lightweight Nodes verify transactions using a process called "simplified payment verification," which allows the Node to determine if a transaction has been included in a Block without having to download the entire Blockchain. *Id.* As this source states, these lightweight Nodes "are effectively placing their trust in full nodes in ensuring that blocks and transactions are being correctly validated against consensus rules." *Id.*

273. *See supra* Section II.7 for discussion of Blockchain Consensus Protocol.

274. *See supra* Section II.7 for an explanation of the issues created with PoW and how PoS attempts to address them. Other alternative protocols are also discussed there.

275. According to Y Combinator, the SAFE was developed after many top startup investors and "is intended to replace convertible notes," preserving their flexibility while avoiding many of their perceived problems. *Startup Documents*, Y COMBINATOR (Feb. 2016), https://perma.cc/USS3-FLM4. The SAFE protocols were so popular in part because Y Combinator open-sourced them in 2015. *Id.*

investor makes a payment in exchange for a contractual right to receive Tokens when certain conditions (often including development of the Token itself) are met.[276] The former head of the fintech practice area at Cooley LLP[277] once stated that the first version of a SAFT he viewed was "toxic" and "a cheap knockoff of the 'Simple Agreement for Future Equity' (SAFE) framework popularized by early stage investor Y Combinator"[278]

Cooley LLP, working in conjunction with Protocol Labs, various Token creators, legal experts, and investors, thereafter announced its own SAFT project in late 2017.[279] The whitepaper on this project[280] explained that its goal was to provide framework that would operate in compliance with existing federal regulations pursuant to which investors would fund development of a network that would generate "genuinely functional utility tokens" that would then be delivered to the investors.[281] The paper readily conceded that the SAFT transaction itself would involve the sale of interests that would be investment contracts under the U.S. securities laws,[282] but the plan was that the resulting utility tokens would not be securities under *SEC v. W.J. Howey, Co.*[283]

---

276. Becky Peterson, *Venture capital has a new way of cashing in on bockchain bonanza—here's what you need to know about SAFTs*, BUSINESS INSIDER (Nov. 19, 2017, 9:00 AM), https://perma.cc/VQ5Y-TDY2. In a SAFT deal, VCs [venture capitalists] invest a certain amount of money in a startup in exchange for its promise to one day give them a set amount of the Tokens it sells in an ICO. *Id.* The agreements are premised on the notion that once the company's service is up and running and consumers are using the Tokens to pay for things on it, those Tokens will become valuable. *Id.*

277. Until recently, Marco Santori was the head of fintech at Cooley LLP, a national law firm with ties to 35% of the U.S. Companies on the Wall Street Journal's Billion Dollar Startup Club list. *See* COOLEY LLP, https://perma.cc/JJG2-7Z89 (claiming that Cooley has worked on "140 life sciences corporate partnering and licensing deals since 2000 with an aggregate value of $38 billion" and worked with more than 190 venture funds credited with raising more than $19 billion in 2015.). Cooley has more than 900 lawyers "across 13 offices in the United States, China and Europe." *Id.* Santori left Cooley to become the president and chief legal officer of Blockchain, a Wallet startup, in February, 2018. Marc Hochstein, *The 'Dean of Blockchain Lawyers' Just Got a New Job*, COINDESK (Feb. 5, 2018, 6:00 PM), https://perma.cc/MXR7-WFUM.

278. Pete Rizzo, *SAFT Arrives: 'Simple' Investor Agreement Aims to Remove ICO Complexities*, COINDESK (Oct. 2, 2017), https://perma.cc/PD9Y-DQMN.

279. *Announcing The SAFT Project*, PROTOCOL LABS BLOG (Oct. 2, 2017), https://perma.cc/DUP2-JJ4K.

280. Juan Batiz-Benet, Jesse Clayburgh, & Marco Santori, *The SAFT Project: Toward a Compliant Token Sale Framework*, PROTOCOL LABS (Oct. 2, 2017), https://perma.cc/EQ8N-E3TJ [hereinafter *SAFT Whitepaper*].

281. *Id.* at 1.

282. *Id.*

283. *Howey* was the 1946 Supreme Court opinion that set out the test for what constitutes an investment contract subject to regulation under the Securities Act of 1933.

While this may be relatively easy to state, it is a profound mistake to believe that the scope and details of the SAFT project are easy to understand. One source apparently took the idea that prefunded utility Tokens[284] might escape regulation as securities upon issuance as evidence that a company with a completed Token with any functional utility probably would not need to worry about the project being a security.[285] This is certainly inconsistent with the position announced by the SEC, which generally treats ICOs as the public sale of securities regardless of whether the Token has a functional utility.[286] Uncertainty about market regulation has led most Token sales, even those in reliance on presale agreements, to be limited to investors from outside the United States.[287]

Before attempting to work with a SAFT, attorneys will need to be able to ascertain whether a client is truly proposing a functional utility Token, and then within that context they will need to evaluate the application of *Howey*.[288] In particular, they will need to consider whether purchasers are

---

SEC v. W.J. Howey Co., 328 U.S. 293, 298–99 (1946). The elements of this test and its potential application to both the SAFT transaction and any resulting functional utility tokens are described in greater detail in the *SAFT Whitepaper*, *supra* note 280, at 6–11.

284. For a consideration of utility Tokens and how regulators regard them, see *supra* note 30 and *infra* note 278.

285. One source describes this as follows:

> If a company has completed development of a token and can distribute tokens at the time of the ICO, then the token is probably not a security and we don't need CoinList or the SAFT. The company can crowdfund via an ICO just like Golem and accept money from anyone. However, if a company is raising funds to develop the token with a promise to distribute tokens to investors in the future, then it is conducting a token presale and not an ICO.

David Gobaud, *ICOs and the SAFT—Why, What, and How* (May 23, 2017), https://perma.cc/EB84-7G2S.

286. Daniel Zinman et al., *SEC Issues Warning to Lawyers on ICOs*, BLOOMBERG LAW, BIG LAW BUSINESS (Feb. 23, 2018), https://perma.cc/6V3K-YQYR. A recent pronouncement from the SEC contained unusually strong warnings directed at attorneys advising clients about cryptotransactions, specifically warning lawyers that "the SEC is laser-focused on them when they advise clients on ICOs." *Id.*

287. As an example, consider the Token presale recently conducted by DFINITY, a Swiss organization, which stated during its offering that "[d]ue to regulatory uncertainty, you must not be a US person by citizenship or residency'" in order to participate. *Frequently Asked Questions*, DFINITY, https://perma.cc/UH8S-WQV5 (last visited Dec. 10, 2018). *See* Gobaud, *supra* note 285.

288. As the SAFT whitepaper notes, "*Howey* is not a black-and-white metric for security status. It is a highly variable facts-and-circumstances test." *SAFT Whitepaper*, *supra* note 280 at 20 (citing U.S. Sec. and Exch. Comm'n, Release No. 81207, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO (July 25, 2017), https://perma.cc/TU8J-W7C2). "[T]he U.S. federal securities law may apply to various activities, including distributed ledger technology, depending on the particular facts

genuinely interested in the underlying usefulness of the Token or its potential for appreciation as an investment. In addition, other regulatory requirements[289] may also impact a client proposal regardless of whether the client contemplates issuance of an interest it calls a "utility Token."[290]

31. Signature

A digital Signature is the mathematical operation used to validate the legitimacy of an electronic message or digital document.[291] In the context of Cryptocurrencies, it is the process through which someone can prove their sole ownership over their Coin, Wallet, etc.[292] The user does this

---

and circumstances, without regard to the form of the organization or technology used to effectuate a particular offer or sale." *SAFT Whitepaper*, *supra* note 280 at 16. ("Whether or not a particular transaction involves the offer and sale of a security—regardless of the terminology used—will depend on the facts and circumstances, including the economic realities of the transaction.").

289. For a very brief discussion of some of the other regulatory requirements, see *infra* Section II.34, II.34.1, II.34.4, and notes 414–16 and accompanying text.

290. As one commentator explains, so-called utility Tokens are designed to "provide users with future access to a product or service." Josiah Wilmoth, *The Difference Between Utility Tokens and Equity Tokens*, STRATEGIC COIN, https://perma.cc/4Y2G-HR4X (last visited Dec. 10, 2018). However, as he notes, while "[u]tility tokens are not designed as investments . . . many people contribute to utility token ICOs with the hope that the value of the tokens will increase as demand for the company's product or service increases." *Id.* It is the intent of the buyer that appears to matter, not the announced intention of the Token's creators. This is certainly the position taken by the SEC when it comes to application of the federal securities laws. Amy Starr, an attorney in the SEC's Division of Corporation Finance, has explained the SEC's position as follows:

> There's a lot been said out there about using utility tokens. Words don't matter in this case. The title doesn't matter. We will look at what it is and if what it is satisfies the Howey test for an investment contract it's a security. If you are buying something that you're only going to use in an already existing platform then I would say hey that token is a use token which may not have the characteristics of the security. There's a spectrum, and where you fall on the spectrum will depend on the facts and circumstances of what you have.

Toju Ometoruwa, *SEC Clarifies Stance Of Security Vs. Utility Tokens*, CRYPTOPOTATO (June 14, 2018), https://perma.cc/D7UN-5754.

The CFTC is in agreement with this approach when it comes to applying commodities regulations. *See* Stan Higgins, *CFTC Aligns With SEC: ICO Tokens Can Be Commodities*, COINDESK (Oct. 17, 2017), https://perma.cc/7J22-3HJZ.

291. "Digital signatures are the most advanced and secure type of electronic signature . . . . [T]hey provide the highest levels of assurance about each signer's identity and the authenticity of the documents they sign." *What are digital signatures?*, ADOBE, https://perma.cc/6EPS-DDTS (last visited Dec. 10, 2018).

292. *See* Axel Hodler, *Proving ownership of a cryptocurrency*, MEDIUM (Aug. 8, 2017), https://perma.cc/KG2U-TGZN.

through use of an asymmetric Key pair: a Public and a Private Key.[293] Used in tandem, the two cryptographic Keys allow the message to be authenticated. To prove that a message is legitimate, the user encrypts the message or transaction data using the Private Key.[294] The user's Public Key is accessible to everyone, so the recipient can decrypt the message.[295] This serves as a digital Signature verification, since only the Private Key could have encrypted that message.

32. Smart Contract

A "Smart Contract" is not really a "contract" at all.[296] Instead, it is (1) pre-programmed logic written in computer code, (2) stored and replicated on a distributed platform or Blockchain, (3) that is executed or run by a network of computers (typically the same computers that host the Blockchain), (4) which results in ledger updates pursuant to the terms of the agreement as specified in the computer code.[297] In other words, "a smart contract enforces a relationship with cryptographic code."[298] A slightly more technical definition was provided by the programmer behind Ethereum, Vitalik Buterin, who explained the Smart Contract approach as starting when

> an asset or currency is transferred into a program "and the program runs this code and at some point it automatically validates a condition and it automatically determines whether the asset should go to one person or back to the

293. *See supra* Section II.25 for an explanation of "Keys" and how they function.

294. Technically, the entire message is not encrypted. Instead, the software creates a hash of the data, and the hash is the digital signatures. "The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing." Margaret Rouse, *digital signature*, TECHTARGET, https://perma.cc/NV2P-3U2E (last visited Dec. 10, 2018); *see also supra* Section II.13 for a discussion of Cryptographic Hashing.

295. For a simplified explanation of public key cryptography, see *What is Public-key Cryptography*, GLOBALSIGN, https://perma.cc/W6JZ-KRTM (last visited Dec. 10, 2018).

296. Andrew Glidden, *Should Smart Contracts Be Legally-Enforceable?*, MEDIUM: BLOCKCHAIN BERKELY BLOG (Feb. 27, 2018), https://perma.cc/G8JP-PFZ6 (noting that Smart Contracts are "not contracts: a contract is essentially an agreement, and agreements live in people's minds, not on hard drives. 'Smart contracts' are really just programmatically-executed transactions (hence, PETs). They're not agreements—they're technology for enforcing agreements.").

297. These elements are essentially isolated in Antony Lewis, *supra* note 80.

298. Alyssa Hertig, *How Do Ethereum Smart Contracts Work?*, COINDESK, https://perma.cc/JX2K-F6SX (last visited Dec. 10, 2018) [hereinafter Hertig, *Smart Contracts*].

> other person, or whether it should be immediately refunded to the person who sent it or some combination thereof."[299]

The potential benefits of Smart Contracts have been widely lauded. They include increased accuracy, transparency, the potential for increased autonomy, a decreased need to "trust" the other parties to an arrangement, automatic backup for data, security for documents as a result of the cryptographic encryption of data, increased speed for transactional processes, and savings since many intermediaries (such as notaries) become unnecessary in the Smart Contract context.[300] The clear intent is that Smart Contracts will be "smart, irrevocable, transparent, and secure."[301] These benefits may be possible in a wide range of situations since Smart Contracts can function as "multi-signature" accounts, manage bilateral agreements, add utility to other contracts, and store records such as registration or membership information.[302] In essence, "smart contracts are programs that execute exactly as they are set up to by their creators."[303]

Bitcoin was the first Smart Contract, "in the sense that the network can transfer value from one person to another. The network of Nodes will only validate transactions if certain conditions are met."[304] Bitcoin can process Bitcoin transactions, but was not designed to execute other kinds of Smart Contracts.[305] Ethereum is currently "the most advanced for coding and processing smart contracts," and has the advantage of being public.[306] On the other hand, a user must pay for computing power with Ether tokens.[307]

The fact that Ethereum is the most advanced platform does not mean that Smart Contracts executed on it are exempt from some potentially

---

299. *See Smart Contracts: The Blockchain Technology That Will Replace Lawyers*, BLOCKGEEKS (2017), https://perma.cc/ZXA9-KC8R.

300. *Id.*

301. Charlie Osborne, *Poor smart contract coding exposes millions of dollars in Ethereum*, ZDNET (Feb. 23, 2018, 12:48 PM), https://perma.cc/PV2X-QQ9Q.

302. *See* Hertig, *Smart Contracts*, *supra* note 298.

303. *Id.*

304. *Id.*

305. *Smart Contracts: The Blockchain Technology That Will Replace Lawyers*, *supra* note 299.

306. The public nature of Ethereum occurs because its coding is all open-source, meaning that it "lets you build your own decentralised apps." Abigail Beall, *What is Ethereum? The open-source crypto platform explained*, ALPHR (June 11, 2108), https://perma.cc/F5TD-3LC4.

307. *Id. Accord* Hertig, *Smart Contracts*, *supra* note 298 (explaining that the language of Etherem is "Turing-complete," meaning that the platform "supports a broader set of computational instructions.").

serious problems. First, there are the problems inherent in setting up an immutable transaction. Those have been explained as follows:

> What happens if I send the wrong code, or . . . I send the right code, but my apartment is condemned (i.e., taken for public use without my consent) before the rental date arrives? If this were the traditional contract, I could rescind it in court, but the blockchain is a different situation. The contract performs, no matter what.[308]

Second, there are the potential regulatory problems. How will governments tax transactions executed via Smart Contract?[309] How will they be regulated?[310] Which agencies and which courts will have jurisdiction?[311] Finally, what happens if there is an error or bug in the code used in a Smart Contract or a weakness that can be exploited by a hacker?[312] Each of these questions raises legal issues about which clients

---

308. *Smart Contracts: The Blockchain Technology That Will Replace Lawyers*, *supra* note 299.

309. Currently, the I.R.S. views all Cryptocurrencies as property, and treats transactions in them as involving the sale and exchange of ordinary property, which means ordinary income will be realized on any gain (and also means the user will need to keep track of any sales or use tax involved.) I.R.S. Notice 2014-21, 2014-16 C.B. 938 [hereinafter *IRS Notice*]. For a consideration of the potential tax consequences associated with Cryptocurrencies, see Zachary B. Johnson, *I Got 988 Problems but Bitcoin Ain't One: The Current Problems Presented by the Internal Revenue Service's Guidance on Virtual Currency*, 47 U. MEM. L. REV. 633, 673 (2016). The I.R.S. announced in March 2014 that "[f]or federal tax purposes, virtual currency is treated as property." *I.R.S. Notice*, *supra* note 309.

310. For a consideration of currently involved regulatory authorities, see *infra* Part III, especially notes 414–22 and accompanying text.

311. These questions have no definitive answer at this point, although at least one court has found that the CFTC has jurisdiction over at least some aspects of Cryptocurrencies. *See infra* note 450.

312. This is far from a hypothetical question. A recent technical assessment of a sample of more than 3000 Smart Contracts hosted on Ethereum has indicated that 89% of the Smart Contracts contained code that could be compromised, and the team of researchers concluded that "[i]f exploited by criminals, these could lead to the theft of roughly $6 million in Ethereum." Osborne, *supra* note 301. The ultimate conclusion based on the total number of Smart Contracts was that there are likely coding bugs in about 34,000 Smart Contracts currently in circulation, leaving millions of dollars' worth of cryptocurrency at risk. *Id.* Note that while this article uses the popular terms of hacking and theft, the reality is that exploitation of the vulnerability is consistent with the code, simply not with the intent behind it. *See, e.g.*, Matt Levine, *Blockchain Company's Smart Contracts Were Dumb*, BLOOMBERG OP. (June 17, 2016), https://www.bloomberg.com/opinion/articles/2016-06-17/blockchain-company-s-smart-contracts-were-dumb (explaining how the infamous hack of The DAO, described *supra* at notes 144–46 and 245–49 and accompanying text, was "allowed" by the terms of the coding published by The DAO, although not by the descriptions of how it was supposed to function found on its website and in other published materials).

may seek advice, making it important that lawyers understand the basics of what a Smart Contract might involve.

33. Software Wallet

While a more complete definition of Wallets in general is found in Definition 37, a Software Wallet is simply the software which allows users to access Cryptocurrency accounts that they own.[313] It is not a tangible item, and does not actually "hold" the user's Crypotcurrencies; it merely allows the owner to access the digital accounts.

34. Tokens

Technically speaking, the difference between a Coin and a Token is that a Coin is a form of Cryptocurrency that operates independently of other platforms.[314] For example, Bitcoin possesses its own independent Blockchain, where transactions relating to Bitcoin are recorded. Altcoins generally work the same way, with each of those Coins having a unique Blockchain on which they operate. Tokens, on the other hand, are built on top of another platform in order to function.[315] For the purposes of regulation, this is a distinction likely to be more form than substance.[316] Regulators are concerned with the functional characteristics of the interests, not necessarily identifying how they operate from a programming standpoint.[317] Therefore, most of this discussion should apply to both Tokens and Coins.

---

313. In somewhat more complicated but precise terms, "Cryptocurrency wallets are software programs that store your public and private keys and interface with various blockchain so users can monitor their balance, send money and conduct other operations." *Cryptocurrency Wallet Guide: A Step-By-Step Tutorial*, BLOCKGEEKS, https://perma.cc/AL6P-AK6F (last visited Dec. 10, 2018).

314. *Difference Between Cryptocurrency Coins and Tokens*, *supra* note 40. Bitcoin, Dash, and Litecoin are identified as examples of Coins. *Id.* On the other hand it is important to remember that this technical distinction may not be appreciated by clients, and even if they fully understand it, they may not use their language this narrowly or precisely. *See supra* notes 102–04 and accompanying text for a brief discussion of the prevalence of imprecise or inconsistent terminology in this context.

315. *Difference Between Cryptocurrency Coins and Tokens*, *supra* note 40.

316. *See* Ometoruwa, *supra* note 290.

317. One source has offered the following explanation of this reality:

> Utility tokens can be used to purchase services on a blockchain network, and they do not offer a financial stake in the underlying business or project. From this basic understanding of a utility token, it would put them outside the scope of the US Securities and Exchange Commission (SEC). Unfortunately, the SEC has previously confirmed that most ICOs for utility tokens should be regarded as securities under the Howey test. It is quite clear that many ICO participants buy

From a regulatory perspective, a Token (or Coin) can fulfill a number of distinct functions, and a single Token can have more than one such purpose.[318] For example, it is possible for a Token to serve as a medium of exchange, like a currency, in which it acts as a payment system between participants.[319] It can act as a digital asset or, in other words, as a digital right; owning this kind of Token can represent ownership of an interest in any kind of property.[320] It can serve as a means of access or membership to a community or group.[321] It can function as a share of or stake in a

---

> tokens in the hope that the value will rise rather than using the token to purchase services on the network.

Paul Costas, *Will the SEC Target Utility Tokens?*, CRYPTODISRUPT (June 15, 2018), https://perma.cc/T2JM-2WWC. Coins usually are not as versatile because they require their own platform rather than being built on top of an existing platform, such as Ethereum, which is designed to support them. *See supra* Section II.19 for an explanation of the Ethereum platform.

318. In fact, by their very nature "Tokens are multi-purpose instruments." William Mougayar, *Tokenomics—A Business Guide to Token Usage, Utility and Value*, MEDIUM (June 10, 2017), https://perma.cc/S3DL-57N3. Coins usually are less versatile because of the expense and difficulty of programming unique Blockchains on which to operate; Tokens solve this by relying on other platforms such as Ethereum. *See supra* Section II.19 for an explanation of the Ethereum platform.

319. Bitcoin certainly functions in this way, which helps explain why it is often viewed as an alternative to Fiat Currency. *Is your Crypto Digital Gold, Gas, or Something Else?*, STEEMIT, https://perma.cc/6ZZY-6YLA (last visited Dec. 10, 2018) ("The first generation of cryptocurrencies were designed as digital Stores of Value. Their purpose was to replace fiat currency as the medium for transactions . . . . Bitcoin is the classic example . . . .") (citing Litecoin, DASH, NEM, Monero, and ZCash as other examples).

320. Perhaps the most obvious examples of these kinds of Tokens or Coins would be gold-based Cryptocurrencies. *A guide to gold-backed cryptocurrency*, GOLDSCAPE.NET (Nov. 24, 2018), https://perma.cc/3YM2-TTFR. For these, "[a] token or coin is issued that represents a value of gold (for example 1 gram of gold equals 1 coin). The gram of gold is stored by a trusted custodian (preferably third party), and can be traded with other coin holders." *Id.*

321. Access Tokens have been described like this:

> Tokens can also play a role of being needed to access the network and pay transaction fees. It's not the sole means of payment—other currencies can be used—but small amounts are needed to use the platform at all. In some ways, Ethereum and all platform blockchains are like this: the native cryptocurrency is just needed to pay gas fees, but people can still transfer (and pay with) meta-tokens. Another example is Melon, which accepts multiple forms of tokens as payment across the network but which also requires that transaction fees be paid in Melon tokens.

Token Rights: Key Considerations in Crypto-Economic Design, SMITH & CROWN (Mar. 30, 2017), https://perma.cc/6UWV-PZMG. Meta-tokens are described as being like a share in the underlying project. *See* Tristan Winters, *Meta-Tokens, ICOs and the Ethereum Blockchain*, ETHNEWS (Sept. 10, 2016), https://perma.cc/9JWE-J5SN.

business venture.[322] It can be a means of rewarding those who contribute to the system.[323] Because there are so many options[324] it is often difficult to appropriately and consistently classify any particular Token, especially because Tokens are often a cross between shares, an internal currency, and accounting units.[325]

Because Tokens are so hard to classify, it is exceedingly difficult to know how they will be regulated. Will they be treated as commodities, currencies, property, securities, or in some other way or under more than one of these regulatory schemes?[326] In order to predict how and when various regulatory authorities may seek to exert control and authority over particular Tokens, it is probably most important to understand them by focusing on whether they have characteristics that are most likely to make them subject to certain forms of regulation.

34.1 Tokens as Commodities

In the U.S., the Commodities Futures Trading Commission (CFTC) regulates the trading in commodities futures, including swaps and forward contracts, and enforces rules against commodities fraud, which covers an incredibly wide range of assets.[327] Not surprisingly, the CFTC has claimed that certain Cryptocurrencies, most notably Bitcoin, are commodities

322. Another way of looking at this kind of Token is to think of it as a tokenized security. Alex Lielacher, *ICO Tokens 101: Understanding Token Types*, BITCOIN MKT. J. (Nov. 21, 2017, 8:00 AM), https://perma.cc/A9E8-HFYL (suggesting that new Tokens from tZero, a portfolio company of Overstock, Inc., would fit this categorization).

323. Bitcoin Miners, for example, receive Coins for successfully solving the mathematical puzzles that are necessary to authenticate Blocks on the Blockchain. *See* Noelle Acheson, *How Bitcoin Mining Works*, COINDESK, https://perma.cc/N4LQ-96PN (last updated Jan. 29, 2018).

324. As of May 15, 2018, there were 738 distinct Tokens listed on Coinmarket, and they had a total capitalization of $57,740,803,913, up from 611 Tokens having a total capitalization of $54,085,903,703 in mid-February. *Top 100 Cryptocurrencies*, *supra* note 1.

325. Pavel Kravchenko, *Know Your Tokens: Not All Crypto Assets Are Created Equal*, COINDESK (Aug. 14, 2017), https://perma.cc/TB67-85UG.

326. See *supra* Sections II.34, II.34.1–34.3 for a consideration of how Tokens are likely to be treated by different regulatory authorities, and notes 427–66 and accompanying text for a brief overview of what that can mean from a regulatory perspective.

327. Commodity regulation may have started in the agricultural sector, but for the last fifty years, the CFTC has had authority over a vast array of financial instruments, including foreign currencies, U.S. and foreign government securities, and U.S. and foreign stock indices. Dennis W. Carlton, *Futures Markets: Their Purpose, Their History, Their Growth, Their Successes and Failures*, 4 J. FUTURES MKTS., 237–71 (1984).

potentially within the ambit of CFTC regulation and enforcement.[328] In early 2018, the CFTC announced an enforcement action against a company and two individuals for the fraudulent offering of a functional Virtual Currency despite the fact that no swap or forward contract was involved.[329] In March of 2018, the District Court for the Eastern District of New York issued an opinion agreeing that the CFTC had jurisdiction over Virtual Currencies.[330]

An affirmative indication of how serious the CFTC is about monitoring cryptotransactions was the recent appointment of two subcommittees by the CFTC Technology Advisory Committee, "one devoted to cryptocurrencies and the other on broader application of distributed ledgers in the finance space."[331] The CFTC has received and considered input from researchers worried about the potential for overregulation in the space,[332] but it continues to be active in seeking to protect investors in this space, especially from false and fraudulent offerings.[333]

34.2 Tokens as Virtual Currencies

The regulatory situation relative to the question of when Tokens might be viewed as "currency" of any type is extraordinarily complex. Speaking

328. In mid-September, 2015, the CFTC determined that Bitcoin and other virtual currencies were commodities, determining that Coinflip had been operating an unregistered commodity option exchange (with Bitcoin as the commodity). *See In re* Coinflip, Inc., CFTC No. 15-29, 2015 WL 5535736 (Sept. 17, 2015). In early 2018, the CFTC issued a "Backgrounder" on Virtual Currency Futures Markets, claiming it had been consistent in asserting jurisdiction over virtual currencies since 2014., *CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets*, U.S. COMMODITY FUTURES TRADING COMMISSION (Jan. 4, 2018), https://perma.cc/7AUW-PTZU.

329. Keith Miller et al., *CFTC Flexes Its Regulatory Muscle in a Case Involving a Virtual Currency*, VIRTUAL CURRENCY REP. (Jan. 29, 2018), https://perma.cc/3BHM-EFTW. In connection with this action, the CFTC obtained from the U.S. District Court for the District of Massachusetts a restraining order and an asset freeze against defendants who had obtained customer funds allegedly without providing any real value. *Id.*

330. Commodity Futures Trading Comm'n v. McDonnell, 287 F. Supp. 3d 213 (E.D.N.Y. 2018).

331. Annaliese Milano, *CFTC to Establish Crypto and DLT Committees*, COINDESK (Feb. 14, 2018), https://perma.cc/TB3U-A7RC.

332. At its February 14, 2018 meeting where the two new subcommittees were announced, the CFTC heard from Brian Knight, a senior research fellow at George Mason University's Mercatus Center, who "raised concerns about the expanding role of regulators in cryptocurrency and blockchain, and said such involvement could prove problematic." *Id.*

333. For a relatively recent exposition about the CFTC's role in regulating Cryptocurrencies, see David Floyd, *CFTC Officials Want Close Cooperation With SEC on Crypto Rules*, COINDESK (May 3, 2018), https://perma.cc/3369-SMGR.

extremely generally, it appears that Virtual Currencies or Cryptocurrencies have not typically been regulated as currencies per se because as of the date the current regulatory positions were being adopted, cryptoassets were neither backed by any government nor accepted as legal tender by any nation.[334] Even without being treated as "real" currencies, companies engaged in Virtual Currency business activities have nonetheless become subject to regulation.[335] Such regulation may be at the state or federal levels, or both.[336]

One of the most problematic areas of regulation for Tokens occurs if the issuer of a Token is treated as being engaged in the business of money-transmission.[337] The issue here is that money-transmission services have been primarily regulated by the states, where the landscape involves an overlapping, conflicting, and often inconsistent set of rules and requirements. Not only are state money transmitter laws complex and time-consuming, the variation between states means that in many cases, a

334. Note that the rationale for treating Cryptocurrencies as something other than "real" currency took a hit in March, 2018, when Venezuela announced it would issue and back a new digital currency known as the Petro. Jack Karsten & Darrell M. West, *Venezuela's "Petro" Undermines Other Cryptocurrencies—and International Sanctions*, BROOKINGS (Mar. 9, 2018), https://perma.cc/9XVS-LAHT. President Trump quickly acted to ban dealing in Petro. Jon Markman, *This Is Why The Venezuela Cryptocurrency Matters*, FORBES (Mar. 20, 2018), https://perma.cc/P583-UR47. Currently, the only international financial institution participating in the distribution of the Petro, in defiance of U.S. sanctions, is the Russian Evrofinance Mosnarbank. Joshua Goodman, *Russia Bank Helps Venezuela Defy US Cryptocurrency Sanctions*, AP NEWS (May 14, 2018), https://perma.cc/3QUN-J3WP. On the other hand, there are reports that other nations, including Russia, Turkey, and Iran, are also looking into developing their own national cryptocurrencies. Karsten & West, *supra* note 334. A second blow to the notion that Cryptocurrencies are not "real" currencies came in the same month when the Marshall Islands became the first country to officially adopt a Virtual Currency as legal tender, alongside the U.S. dollar. Hilary Hosia & Nick Perry, *This Is the First Country to Adopt a Cryptocurrency as its Official Currency*, MONEY (Mar. 5, 2018) (on file with the Campbell Law Review).

335. For the past several years, the U.S. Department of the Treasury Financial Crimes Enforcement Network ("FinCEN") has accepted that virtual currency is not a "currency" under regulations implementing the Bank Secrecy Act because it is not legal tender, but FinCEN nonetheless subjects certain Virtual Currency businesses to regulation, including rules for money services businesses acting as money transmitters. John L. Douglas, *New Wine into Old Bottles: Fintech Meets the Bank Regulatory World*, 20 N.C. BANKING INST. 17, 65 (2016).

336. *See infra* notes 427–66 and accompanying text.

337. The Chairmen of both the CFTC and SEC "have identified state money transmission law as a potential barrier" to cryptotransactions. Jerry Brito, *How the SEC and CFTC can Address Cryptocurrency While Preserving U.S. Innovation*, COIN CTR. (Jan. 25, 2018), https://perma.cc/6GC5-GDKW.

business seeking to operate across state lines will need to comply with burdensome requirements that differ from jurisdiction to jurisdiction, although a handful of states are trying to be very welcoming to crypto-based enterprises.[338]

Federal banking laws can apply as well, and certain activities can bring companies involved in cryptotransactions under the Bank Secrecy Act, which can require the collection, retention, and reporting of customer information with FinCEN.[339] The consequences of non-compliance with these requirements can be significant.[340]

34.3 Tokens as Property

Although the CFTC treats Cryptocurrencies as commodities, and Banking authorities see them more as currencies, the I.R.S. announced in March 2014 that "[f]or federal tax purposes, virtual currency is treated as

338. Jonas Borchgrevink, *Money Transmitter Licenses: Do You Need One for Your Bitcoin Business?*, CCN (Feb. 18, 2014), https://perma.cc/M69M-D92U (noting that obtaining a money transmitter license "is both an expensive and lengthy process. It can take multiple years to be approved for such a license." This is particularly problematic given the lack of clarity in U.S. regulations). Note also that some states have affirmatively exempted Cryptocurrencies from their money transmitter licensing requirements, although this is far from a universal approach. Felix Shipkevich, *Under New Crypto-Friendly Laws, Virtual Currency Exempt from Taxes in Wyoming*, MONEY TRANSMITTER L. (Apr. 3, 2018), https://perma.cc/3Z5C-6JAH. Wyoming is the trailblazer in this area, exempting Virtual Currencies from state money transmitter laws, state taxation, and even state securities laws (unless the interest is specifically marketed as an investment). *Id.* For a description of the various rules in place in different states, see Carlton Fields, *State Regulations On Virtual Currency and Blockchain Technologies*, JDSUPRA (Nov. 10, 2017), https://perma.cc/TL9W-7NDX.

339. Douglas, *supra* note 335, at 43 (noting that "a person operating a platform for the exchange of virtual currencies to real currencies would be subject to regulation as [a Money Services Business], as would a person operating a payment system that allows merchants to receive payments in virtual currencies from their customers."). The concern is that organized crime or terrorist organizations might use virtual currencies to "launder" money or support terrorist activities, which explains why AML (Anti Money Laundering) and KYC (Know Your Customer) requirements might be enforced against companies that may be facilitating such transactions. Saurabh Chhabra, *What is KYC and AML? Why it's so Important in Cryptocurrencies?*, COINGAPE (Mar. 20, 2018), https://perma.cc/6WEL-WDQH.

340. Peter Van Valkenburgh, *Securities Laws Aren't the Only Rules Token Sales Have to Consider*, COINDESK (May 20, 2017), https://perma.cc/3XPL-U5RE. In other contexts, particularly in the settlement agreement they reached with Ripple in 2015, FinCEN has suggested that selling a token (XRP in the Ripple case) is money transmission, and to do so without registering with FinCEN and complying with its regulations is a serious offense worthy of a major monetary penalty ($700,000 in the case of Ripple) or else time in jail for company management and even potentially shareholders. *Id.*

property."[341] Some state tax authorities have followed suit.[342] Thus, purchases and sales of Bitcoins and payments made with Bitcoins (and other Virtual Currencies as well) can be taxable events, as demonstrated in the following illustration:

> For example, if Sally buys a cup of coffee at Starbucks for $4.00, but pays for the coffee using a digital currency she acquired at a cost of $2.00, she has realized a $2.00 capital gain on the transaction. Even more interesting is that there could not only be a sales tax imposed on Starbucks for the sale of the coffee, Sally could perhaps be deemed to have sold her digital currency for the $4.00 cup of coffee and owe sales tax on her sale as well. The recordkeeping and compliance costs seem overwhelming (and as a result, are perhaps most often ignored), but this seems to be the logical outgrowth of the IRS position.[343]

The reality is that Tokens or Coins that are convertible into Fiat currency or real world goods (directly or indirectly) are treated as property by the I.R.S., regardless of how they are classified under other regulatory schemes.[344]

One additional piece of information on the tax front is also important. Prior to this year, many Cryptocurrency investors relied on section 1031 of the Tax Code to allow tax-free conversions between different kinds of Cryptocurrencies, but the recent changes to federal tax law have removed this as a possibility by limiting 1031 exchanges to real estate.[345]

---

341. *I.R.S. Notice, supra* note 309.

342. Douglas, *supra* note 335, at 44–45 (citing both New York and Washington state rulings on this issue). Wyoming, on the other hand, has chosen to exempt cryptocurrencies from taxation in that state. Shipkevich, *supra* note 338.

343. *I.R.S. Notice, supra* note 309, at § 4 (answering Frequently Asked Questions: Q.3 (receipt as payment for goods or services), Q.6 (gain or loss on exchange), Q.8 (payment for Mining), Q.10 (payment to independent contractor), & Q.11 (wages for employment)). The illustration comes from Douglas, *supra* note 335 at 55.

344. Austin Mills, *Do Token Sales Have Special Tax Considerations? And Other Blockchain Legal Implications*, HYPEPOTAMUS (Nov. 8, 2017), https://perma.cc/V8YP-77QW (appearing to suggest a false dichotomy, suggesting that this tax classification applies "where the token is not a security"). In actuality, the Token could easily be both a security and subject to this kind of tax treatment, as there is no tax-free exchange rule for Tokens or Coins, as there often is for equity investment. Robert W. Wood, *Loophole Allows Tax-Free Bitcoin Exchanges into 2018*, FORBES (Dec. 28, 2017, 08:47 AM), https://perma.cc/EZU3-3XDX.

345. I.R.C. section 1031 allows a swap on one like-kind business or investment asset for another. Wood, *supra* note 344. Although most swaps are taxable sales, this provision contains a limited exception to that rule. *Id.* Because the I.R.S. classified cryptocurrencies as property "many investors assumed that meant you could swap them tax-free under section 1031." *Id.* The massive tax bill passed at the end of 2017 eliminated that argument going forward, by limiting like-kind exchanges to real estate. *Id.* While there may be a

34.4 Tokens as Securities

The sale of securities within the U.S. is generally within the purview of the Securities Exchange Commission (SEC),[346] and the SEC has indicated that it fully intends to exercise its jurisdictional powers when it comes to Tokenized offerings, regardless of whether a particular Token is characterized as a "utility" interest or otherwise.[347] The appropriate analysis is whether the underlying Token is an investment contract, as such term has been defined by the courts.[348]

The applicable test basically looks at these factors: (i) whether there exists an investment of money (or something else of value), (ii) whether there exists a common enterprise, (iii) whether there exists an expectation of profits, and (iv) whether the expectation of profits is from the essential entrepreneurial efforts of others.[349] Thus, a Token that might be classified as an investment, as a security, as being share-like,[350] or as being an equity token,[351] is highly likely to be regulated as a security. It is, however, worth emphasizing that merely calling something a "utility" Token is not at all likely to render it exempt from regulation by the SEC.[352] None of the elements of the *Howey* investment contract analysis inquire as to the underlying function or "utility" of the interest being sold. Instead, the focus is very much on the motivations of the issuer and investor, and the relationship between the two.[353]

---

limited transitional exceptions, investors in Cryptocurrencies will need to understand the new rules moving forward. *See id.*

346. It is illegal to offer or sell securities in the U.S. unless both the offer and sale are exempt or made pursuant to an effective registration statement. Securities Act of 1933, 15 U.S.C. §§ 3(a)(11), 77d, 77e(a), (c) (2012). While there is an exemption within the Securities Exchange Act of 1933 for offerings that take place wholly within a single state, most Token sales are not likely to be so limited. *See Intrastate Offerings*, U.S. SEC. & EXCH. COMM'N, https://perma.cc/5RK8-47N4. The instrastate offering exemption is found in section 3(a)(11) of the Securities Act of 1933, but its requirements are stringent. *See id.*

347. On February 6, 2018, the Senate heard testimony from SEC Chairman Jay Clayton that "every ICO token the SEC has seen so far is considered a security and explained that if a crypto-asset issued by a company increases in value over time depending on the performance of the company, it is considered a security." Young, *supra* note 33.

348. The definition of "investment contract" originated in the U.S. Supreme Court opinion in *SEC v. W.J. Howey Co.*, 328 U.S. 293, 298–99 (1946).

349. Consider the SAFT Whitepaper. *SAFT Whitepaper*, *supra* note 280, at 6–11.

350. These first three categories are part of the classification structure proposed by Euler. Euler, *supra* note 38.

351. Steemit used this as one of its potential categories. Basiccrypto, *supra* note 38.

352. *See* Young, *supra* note 33.

353. This is reflected in the SEC's approach to how to regulate Cryptocurrencies. *See* Wilmoth, *supra* note 126.

35. Uniform Regulation of Virtual-Currency Businesses Act

The Uniform Regulation of Virtual-Currency Businesses Act (Uniform Act) was released by the Uniform Law Commission (ULC)[354] on October 9, 2017, after having been approved at the annual meeting in July of that year.[355] Although as of May 2018, no state had enacted the Uniform Act, it was under consideration in three states.[356] Moreover, past experience indicates that uniform legislation promulgated by ULC is often influential on state legislators.[357]

One of the stated goals of the Uniform Act is to provide "a balanced and reasonable regulatory structure that should validate good business practice and thus enhance trust for users of virtual currency, and may lead to SEC approval of virtual-currency offerings."[358] The Uniform Act is also clearly drafted with both state money transmission laws and Financial Crimes Enforcement Network (FinCEN) money services business regulations in mind, with the express observation that the Uniform Act provides protections and obligations that are generally similar to those legal regimes.[359]

In essence, with certain exemptions, the Uniform Act requires a license in order for a business to legally "engage in virtual-currency business activity" or to hold oneself out as doing so.[360] This includes "exchanging, transferring, or storing virtual currency or engaging in virtual-currency administration . . . ."[361] "Virtual Currency" is defined as a digital representation that "(i) is used as a medium of exchange, unit of account, or store of value; and (ii) is not legal tender, whether or not

354. The ULC, formerly known as the National Conference of Commissioners on Uniform State Laws (NCCUSL), has as its mission the goal of providing "states with non-partisan, well conceived, and well drafted legislation that brings clarity and stability to critical areas of state statutory law." UNIF. ACT *supra* note 13.

355. The full text of the Uniform Act along with a detailed prefatory note and commentary following each of the substantive sections is available online. *See id.*

356. Connecticut, Hawaii, and Nebraska were considering the Uniform Act as of May 15, 2018. *See* UNIF. ACT, *supra* note 13.

357. Jeremy M. McLaughlin & Eric A. Love, *K&L Gates Discusses the Virtual-Currency Businesses Act and Coming Cryptocurrency Regulation*, CLS BLUE SKY BLOG (Nov. 17, 2017), https://perma.cc/E3GE-AFGM (noting that it "is not unusual for multiple states to adopt the ULC legislation.").

358. UNIF. ACT, *supra* note 13, Prefatory Note at 12.

359. *Id.* at 1–2.

360. *Id.* at § 201.

361. *Id.* at § 102(25). Interests in precious metal and exchanging digital representations of value within an online game or gaming platform can also be regulated under certain circumstances. *Id.*

denominated in legal tender."[362] Notwithstanding this very broad definition, "Virtual Currency" specifically does not include non-convertible merchant affinity or rewards interests or most representations of value limited to online games.[363] The definitions for exchanging,[364] transferring,[365] or storing[366] of Virtual Currency all require the business to be exercising "control" over the particular activity on behalf of someone other than the "owner," and the definition of control means that the business must have the power to unilaterally execute or prevent a Virtual Currency transaction.[367] The definition of "Virtual Currency Administration" means the power to issue the Virtual Currency with authority to redeem it for legal tender, bank credit, or other Virtual Currency.[368]

There are some exemptions built into the Act, including a three-tiered system of regulation designed to allow businesses to "ramp up" their activities before obtaining the license described in the Uniform Act.[369] However, the first tier (which would exempt a business from licensure) is limited to businesses whose Virtual Currency business activity within a state "is reasonably expected to be valued, in the aggregate [within that state], on an annual basis at $5,000 or less . . . ."[370] The second tier allows a business to register rather than obtaining a license, but it is limited to entities whose annual Virtual Currency activity in the state is not expected to exceed $35,000.[371] In addition to the relatively low dollar limit, the registration requirements are similar to the licensure requirements in several respects.[372] The option is only available for two years, after which

362. *Id.* at § 102(23)(A).

363. *Id.* at § 102(23)(B). These definitions were apparently adopted to ensure that the Uniform Act tracks FinCEN treatment of virtual currencies. *See id.* at § 102, comments (citing an unpublished FinCEN no-action letter dated April 2016, on file with the ULC).

364. *Id.* at § 102(5).

365. *Id.* at § 102(21).

366. *Id.* at § 102(20).

367. *Id.* at § 102(3).

368. *Id.* at § 102(24).

369. The "on-ramp" terminology originates with the ULC, which claims that the tiered system and relatively black-line approach provides businesses with clear requirements for what the business must do to comply while also allowing some "testing of the products and services in the enacting state." *Id.* at § 103, comment 2.

370. *Id.* at § 103(b)(8).

371. *Id.* at §207 at comment 4.

372. *Id.* at § 207(a). As for points of commonality, both a registrant and licensed company must meet the minimum net worth requirements and reserves, and provide evidence that it has policies and procedures to comply with the Bank Secrecy Act, as well as the Uniform Act's examination and disclosure requirements. *Id.* at §§ 207(a)(6)–(8).

the entity must cease its Virtual Currency business or apply for a license even if it will not exceed annual in-state earnings of $35,000.[373]

The Act does include several exemptions that appear to mirror most common exemptions in state money transmission statutes. Among these are exemptions for government agencies, banks (including the OCC's proposed special purpose national bank,[374] but not Industrial Loan Companies), entities providing processing or clearing services, and persons using Virtual Currency on their own behalf, for personal, family, or household purposes, or for academic purposes.[375] Entities that are licensed under the state's money transmission statute and which have obtained permission to engage in Virtual Currency activities need not be licensed under the Uniform Act, although they must comply with certain of its provisions.[376]

There are other exemptions from the licensing requirements, including exemptions for any person who only provides processing, clearing, or settlement services to exempt Virtual Currency businesses;[377] and any person who "contributes only connectivity software or computing power to a decentralized virtual currency, or to a protocol governing transfer of the digital representation of value," or who "provides only data storage or security services" for a Virtual Currency business.[378] Other exemptions exist for dealers in foreign exchange, attorneys, and title insurance companies providing escrow services, securities or commodities intermediaries, secured creditors, Virtual Currency control-services vendors, and persons that do not charge for their Virtual Currency business activities.[379] The Act also exempts any Virtual Currency transaction that is

373. *Id.* at § 207(d)(4).

374. In December of 2016, the Office of the Comptroller of the Currency announced that it is exploring the possibility of special purpose national bank charters for Fintech companies. OFFICE OF THE COMPTROLLER OF THE CURRENCY, EXPLORING SPECIAL PURPOSE NATIONAL BANK CHARTERS FOR FINTECH COMPANIES (Dec. 2016), https://perma.cc/X9B3-FQWL. Comments were not uniformly positive. *See* Hannah Levitt, *OCC's Fintech Charter Plan Draws Debate*, MARKET WATCH (June 23, 2017) (on file with Campbell Law Review). Despite litigation from state regulators who see the plan as usurping state authority, the OCC has not abandoned this as a possibility, and discussion about the viability and desirability of special charter Fintech banks continues. *See* Kevin Petrasic et al., *Fintech Companies and Bank Charters: Options and Considerations for 2018*, WHITE & CASE (Jan. 10, 2018), https://perma.cc/QT4S-HXKG.

375. UNIF. ACT, *supra* note 13, at §§ 103(1), (2), (4), (7).

376. *Id.* at § 103(b)(3).

377. *Id.* at § 103(b)(4).

378. *Id.* at § 103(b)(6)(A)–(B).

379. *Id.* at §§ 103(b)(5), (9)–(14).

subject to the Electronic Fund Transfer Act, the Securities Exchange Act of 1934, or the Commodities Exchange Act.[380]

For companies engaged in Virtual Currency business activities without an exemption, however, the licensing requirements are extensive. The application process requires a detailed application covering a wide variety of information about the business, all of its executive officers,[381] its funds, and various licenses that the business may be required to hold.[382]

There are a number of additional requirements that appear related to, but in some respects different from, traditional state regulations. The Uniform Act requires applicants to deposit security with the state to secure performance of its duties, but the amounts and kinds of security that can be used vary and may include funds or investment property, a letter of credit, a surety bond, or other security satisfactory to the state.[383] States may permit Virtual Currency to meet the requirement in a variety of ways.[384] The Uniform Act also includes minimum net worth standards and requires applicants to maintain sufficient unencumbered reserves to wind down operations.[385] The Uniform Act imposes recordkeeping,[386] reporting,[387] and requirements that are similar to state money transmitter laws. Applicants are required to have satisfactory policies and procedures and to implement a compliance program.[388] Finally, licensees (and registrants)[389] must make numerous disclosures to residents regarding fees and charges,

380. *Id.* at § 103(b).

381. "Executive officer" is defined as a "director, officer, manager, managing member, partner, or trustee of a person that is not an individual." *Id.* at § 102(6).

382. *Id.* at § 202.

383. *Id.* at § 204.

384. *Id.* at comment 1, 5. Apparently this was deemed important because of the difficulty that some Virtual Currency business might have in obtaining surety bonds or other traditional forms of security.

385. *Id.* at § 204(b). The applicant can use Virtual Currency, not including Virtual Currency over which it has control on behalf of a resident, to meet the net worth requirement. *Id.* at § 204(c).

386. Required recordkeeping obligations are set out in the Uniform Act. *Id.* at § 302.

387. *Id.* at §305 (mandating interim reports).

388. *Id.* at §§ 601–602. These include "policies and procedures for (1) an information-security and operational-security program; (2) a business-continuity program; (3) a disaster-recovery program; (4) an anti-fraud program; (5) an anti-money-laundering program; (6) a program to prevent funding of terrorist activity; and (7) a program designed to ensure compliance with" all other relevant state and federal law. *Id.* at § 601(a).

389. See *id.* at §§ 102(3),(5),(20),(21),(23)(a)–(b),(24),(25), 201 and accompanying text for a description of registrants.

insurance, and error resolution rights before establishing a "relationship" with them.[390]

The Uniform Act does include enforcement provisions for material violations of the Act's provisions.[391] It also permits actions against people who "engage[] in an unsafe or unsound act or practice," and "an unfair or deceptive act or practice."[392] The Act does, however, provide only a very limited private right of action.[393]

36. Virtual Currency

From a regulatory standpoint, "Virtual Currency" probably should be understood as being more precise than "Cryptocurrency," which is a phrase of variable meanings that can be used to cover all Coins and Tokens.[394] Most of the existing regulatory authorities, and the Uniform Act proposed by the Uniform Law Commission, use the term "Virtual Currency" to describe what is being regulated.[395] Unfortunately, just as is the case with the word "Cryptocurrency," there is less than complete agreement among these authorities as to what "Virtual Currency" means.[396]

Not surprisingly, the definitions vary most significantly depending on the background in which the applicable regulatory authority is acting. Consider the I.R.S., which is charged with helping taxpayers "understand and meet their tax responsibilities and enforce the law with integrity and

390. *Id.* at § 501.

391. *Id.* at § 402(a)(1).

392. *Id.* at § 402(a)(3).

393. *Id.* at § 407. Comment 1 suggests that there may be a private right of action under section 502 for a person acting as a securities intermediator who violates U.C.C. § 8–503, and Comment 2 says that the other exception may be for section 502 violations that involve fraudulent acts, "such as fraudulently covering up a failure to maintain the required amount of virtual currency under control, or converting for the virtual-currency business' own use the virtual currency under its control for other persons." *Id.* at comment 1–2.

394. *See supra* Section II.12 (discussing of the potential meanings of Cryptocurrency).

395. The Uniform Regulation of Virtual Currency Businesses Act is discussed in some detail *supra* Section II.35. *See infra* note 408 for the definition it employs. For other definitions, *see infra* notes 398 (I.R.S. definition); 401 (FinCEN definition); 404 (Conference of State Banking Commissioners' definition); and 406 (N.Y. Department of Financial Services Definition).

396. As one observer noted, "[t]here's a lot of misunderstanding around the terms "virtual" and "digital," and people often mistakenly use them interchangeably." Andrew Wagner, *Digital vs. Virtual Currencies*, BITCOIN MAG., Issue 22 (May 2014), at 1. https://perma.cc/NRL9-JWVQ.

fairness to all."[397] The I.R.S. uses the following definition of Virtual Currency:

> Virtual currency is a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value. In some environments, it operates like "real" currency—i.e., the coin and paper money of the United States or of any other country that is designated as legal tender, circulates, and is customarily used and accepted as a medium of exchange in the country of issuance—but it does not have legal tender status in any jurisdiction.[398]

While the I.R.S. stated that Virtual Currency does not have legal status, as of March 2018 that is no longer completely accurate,[399] although no American state recognizes it as such. Regardless of this particular development, treating Virtual Currency as property allows the I.R.S. to maximize certain taxes, by denying taxpayers favored rates that might have been applicable if Virtual Currency was treated like foreign currencies.[400]

On the other hand, banking authorities tend to have a significant interest in regulating Virtual Currencies as currencies. For example, the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) defines "Virtual Currency" to be "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency."[401] FinCEN's guidance is limited to convertible Virtual Currencies, which means Virtual Currency that "either has an equivalent value in real currency, or acts as a substitute for real currency,"[402] and was issued despite the fact that when that guidance was

397. I.R.S., *The Agency, Its Mission and Statutory Authority* (June 27, 2018), https://perma.cc/D9AJ-A7XS.

398. *Internal Revenue Bulletin: 2014-16*, I.R.S. (Apr. 14, 2014). This definition was the basis for the I.R.S.' pronouncement in its "Virtual Currency Guidance" that "virtual currency is treated as property for U.S. federal tax purposes." I.R.S., *IRS Virtual Currency Guidance* (Mar. 25, 2014), https://perma.cc/S6UD-D68M.

399. It is still not legal tender in any American jurisdiction. *IRS Virtual Currency Guidance*, *supra* note 398. History can provide other examples of "currency" that were not considered "legal tender" in this country. Two of such examples are military scrip and depression scrip. *See generally* Loren Gatch, *Local Money in the United States During the Great Depression*, 26 ESSAYS IN ECON. & BUS. HIST. 47 (2008). As of the date this article was being revised, only the Marshall Islands had accepted any Cryptocurrency as legal tender. *See* Hosia & Perry, *supra* note 334.

400. *See supra* Sections II.34.2 and II.34.3 for a brief discussion of this issue.

401. U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, FIN-2013-G001, *supra* note 21.

402. *Id.*

issued, "Virtual Currency [did] . . . not have legal tender status in any jurisdiction."[403]

State Banking authorities, again not surprisingly, take an approach similar to that used by FinCEN. For example, the Conference of State Bank Supervisors (CSBS) has determined that, for its purposes:

> Virtual Currency is a digital representation of value used as a medium of exchange, a unit of account, or a store of value, but does not have legal tender status as recognized by the United States Government. Virtual Currency does not include the software or protocols governing the transfer of the digital representation of value. Virtual Currency does not include stored value redeemable exclusively in goods or services limited to transactions involving a defined merchant, such as rewards programs.[404]

This definition builds in certain exclusions, probably in recognition of the limits of state banking authorities' power.

The New York Department of Financial Services took an extraordinarily broad approach to what is meant by Virtual Currencies, carving out limited exceptions from the scope of specialized regulations governing Virtual Currencies in that state.[405] Under the New York regulations,

> 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.[406]

Certain narrow exclusions are carved out from this definition, so that "Virtual Currency" as used in those regulations does not include digital units that are: (1) non-convertible and non-redeemable, and are designed to be used solely within online gaming platforms; (2) issued as part of loyalty or rewards program that can only be used with the issuer or designated merchants as part of that program; or (3) used as part of prepaid cards.[407]

The ULC's proposed Uniform Regulation of Virtual Currency Businesses Act (the Uniform Act) (see Definition 35 for more information), was written at least partially to provide a tiered-system of regulation rather than the one-size-fits all approach of the New York

403. *Id.* This still holds true within the U.S., but is no longer universally true. *See* Hosia & Perry, *supra* note 334 (discussing the Marshall Islands).

404. CONFERENCE OF STATE BANK SUPERVISORS, STATE REGULATORY REQUIREMENTS FOR VIRTUAL CURRENCY ACTIVITIES (Sept. 15, 2015).

405. 23 N.Y. FIN. SERV. LAW § 200.2(p) at 5–6.

406. *Id.*

407. *Id.*

provision.[408] The Uniform Act says that Virtual Currency means "a digital representation of value that: (i) is used as a medium of exchange, unit of account, or store of value; and (ii) is not legal tender, whether or not denominated in legal tender," excluding both merchants' affinity or rewards programs that cannot be "taken from or exchanged with the merchant for legal tender, bank credit, or virtual currency" and any "digital representation of value issued by or on behalf of a publisher and used solely within an online game, game platform, or family of games sold by the same publisher or offered on the same game platform."[409] In the view of the drafters of the ULC, "Virtual currencies are a subset of cryptocurrencies."[410]

Two commentators who have considered the scope of regulations affecting various Cryptocurrencies take a slightly different approach, concluding that "[a] subset of virtual currency is 'cryptocurrency,' by which we mean an internet-based virtual currency in which the ownership of a particular unit of value is validated using cryptography."[411] They use "Virtual Currency" "to refer to a medium of exchange existing entirely in intangible form that is not legal tender but which can substitute for legal tender."[412] They contrast modern Virtual Currencies with the way in which the term was originally used, where not only did the term imply that the units in question exist "only in an electronic or digital form," but also that they were only used "as a medium of exchange between members of an online or virtual currency community," for example in online games, on social media, or to purchase virtual goods or prizes in loyalty programs.[413] They note that currently, these original uses are generally exempted from Virtual Currency regulations.

37. Wallet

A Cryptocurrency Wallet does not work precisely like an everyday wallet for Fiat currencies that are carried around in a pocket or purse. By their nature, Cryptocurrencies do not have a tangible form and instead exist

408. UNIF. ACT, *supra* note 13, Prefatory Note at 2 (touting the Uniform Act's "three-tier system for determining which providers are exempt from the act consisting of persons engaging in only minor activity, an intermediate registration status that is modeled as an 'on-ramp' or 'regulatory sandbox' that is designed to facilitate innovations in virtual-currency businesses with more modest regulatory requirements, and full licensure for providers with specified business volumes.").

409. *Id.* at 17.

410. *Id.* at 4.

411. *Advancing*, *supra* note 63, at 504.

412. *Id.*

413. *Id.*

only as Blocks on a digital Blockchain. As such, they cannot be removed and stored anywhere else. Instead, a Cryptocurrency Wallet stores the secure digital codes necessary to access the Blockchain. Similar to an online banking PIN, these digital codes (known as Private Keys), will demonstrate ownership of a public digital code (the Public Key) that then enables the user to access the currency addresses. "Once your private key matches the public key, you may access and use your currency."[414]

The most secure form of Wallets are hardware, such as TREZOR, LedgerWallet and Keepkey.[415] Hardware Wallets are a form of "Cold Storage," which means that the information in them is stored apart from the web and is therefore inaccessible to hackers or others as long as the hardware is not connected.[416] In addition, even after being connected, Hardware Wallets contain an additional level of security. They "have a secure chip in them (or equivalent) that means when you connect them to a computer to send your currency you never need to input your private key on the computer itself. You simply input a pin code on the piece of hardware, meaning that trading on a compromised computer is safer."[417] The downside to Hardware Wallets is the expense[418] and the difficulty in deciding which qualities to pay for.[419]

---

414. Oliver Dale, *Best Bitcoin Wallets 2018: Hardware vs Software vs Paper,* BLOCKONOMI (July 17, 2018), https://perma.cc/XSC5-S4XN [hereinafter *Wallets*].

415. These are three of the most popular hardware Wallets. *Id.*; *see also* Ofir Beigel, *Best Bitcoin Wallet Reviews and Comparison for 2018*, 99BITCOINS, https://perma.cc/J5Y3-B6MQ. See *supra* Section II.23 for more discussion of Hardware Wallets.

416. *See* Redactor, *supra* note 268 (explaining that for a Hardware Wallet, "[y]ou need to plug in the hardware device to any internet connected device, enter your pin and transact. These help users transact online and at the same time enable them to keep their currencies away from danger.").

417. *Wallets*, *supra* note 414. In addition, "[i]f the hardware breaks or is lost, then you can restore your access to your currency on a new device from the 'seed words' you receive with your hardware wallet (i.e., a string of random words used to restore your wallet and recover your currency)." *Id.*

418. One source suggests that the "Ledger Nano S is the cheapest of the three hardware wallets with a screen; it costs about $95. Ledger, one of the most well-known Bitcoin security companies, released the device in August 2016." Jordan Tuwiner, *Which is the Best Bitcoin Wallet?*, BUY BITCOIN WORLDWIDE, https://perma.cc/S4Z9-UK6N. The Nano Blue costs about four times as much, pricing the two wallets in Euros, at €70 for the Ledger Nano S and €275 for the Blue. Romain Dillet, *Ledger Grabs $7 Million for its Cryptocurrency Hardware Wallets*, TECHCRUNCH (Mar. 30, 2017), https://perma.cc/C4NM-EAA5.

419. As one commentator explained, "[a]n all-in-one package wallet does not exist. It is important that you manage to find the wallet that addresses your greatest concern, be it security from theft, ease of transfer, convenience, monetary cost, or even style." Suji Velu, *How To Keep Your Cryptocurrency Safe: 7 Must Have Wallets*, BLOCKGEEKS, https://perma.cc/RG7F-DQQ6.

Software Wallets[420] can be free or available at very low cost and may therefore be the best choice for someone storing only a small amount of Coins.[421] Software Wallets may be desktop computer programs that store Cryptocurrency locally on your PC or laptop (which is very convenient but leaves security entirely up to the user). Mobile Wallets operate through an app on a smart phone. This is also incredibly convenient but not necessarily as secure as someone with a significant amount of Cryptocurrency is likely to prefer. Finally, software Wallets can be online.[422] These web-based Wallets are even more convenient since they can be accessed anywhere and can be linked to desktops or mobile devices.[423] On the downside, the Private Keys are stored by the website owners rather than the currency owner.[424] This requires a lot of trust in the Wallet owner and the level of security that they maintain.[425]

III. CONCLUSIONS

Talking to clients or potential clients about their interest in Cryptocurrencies, Tokens, or other Blockchain technologies in their business operations is undoubtedly going to be challenging. For a variety of reasons, clients may be quite enthusiastic about the possibilities that these recent developments offer. Putting aside for the moment those clients who simply wish to exploit the lack of clear regulations for personal gain,

420. See *supra* Section II.33 for more discussion of Software Wallets.

421. *See* Brad Stephenson, *The 7 Best Bitcoin Hardware and Software Wallets*, LIFEWIRE (Jan. 28, 2018) https://perma.cc/762G-QGNP (noting that "Software wallets are usually used for making smaller transactions . . . .").

422. This article uses relatively basic terminology, and already new labels are appearing. One source, for example, breaks Wallets into all of the following categories: Hardware Wallets, paper wallets, mobile wallets, desktop wallets, web wallets, multisig wallets, SPV wallets, and brain wallets. Beigel, *supra* note 415. In essence, though, this listing includes "wallet[s] installed on a computer connected to the Internet, or even a wallet installed on your mobile phone, assuming you have an active data connection to and from your phone." *Id.*

423. *Id.*

424. "[W]eb wallets are the least secure option for storing bitcoins because the operators own the private key to the bitcoins stored on their site. You're basically asking someone else to hold your coins for you." *Id.*

425. One of the earliest publicized incidents of Bitcoin hacking involved a Wallet service. *See* Lee, *supra* note 57, and accompanying text (discussing the hacking of MyBitcoins Wallet service). For additional details about the kinds of Wallets, see *Wallets, supra* note 414. Dale also notes that some Wallets can store multiple currencies, while others are designed to store only one. *Id.* Some require you to download the code to your device; others provide that most of the processing power required is carried out by network servers. *Id.*

or those hoping to trick the unwary or unsophisticated into backing unsupportable ventures, there are some extraordinarily good reasons why clients may be passionate about the topics identified in this article.

Some of them will buy into the vision behind Bitcoin and Blockchain. Imagine an open-source (transparent), decentralized (democratic), immutable (incorruptible), truly international (not tied to any one government or nation) medium of exchange. Money laundering and fraudulent transfers of assets or illegal payments would be impossible if the underlying transactions were transparent and subject to inspection. Governments and large institutions could not interfere in the decisions being made on the Blockchain. Clients with this mindset may be seeking advice about how to become part of the Cryptocurrency and Blockchain world, without running afoul of the various regulations that may come into play.

Other clients are likely to be more intrigued with the possibilities for profiting from the new technology. They may want advice as to the legality of additional sources of funding or legal input as to the potential ramifications of innovative uses of Blockchain technology. Clients with this mindset may have legitimate and perhaps even revolutionary ideas, although some may simply want to appear trendy.

Of course there will be those who will be attracted by the sheer amount of money involved. These clients in particular are likely to benefit from cautionary advice about the many pitfalls associated with conflicting and rapidly developing regulations. Without competent legal advice, the risks may outweigh the benefits of participation in these developments. On the other hand, clients will not want to look back in a few years to find themselves on the list of persons with the "Worst Technology Predictions of All Time" because they missed out on Blockchain, Decentralized Ledgers, or other cryptotransactions.[426]

426. Robert Strohmeyer, *The 7 Worst Tech Predictions of All Time*, PC WORLD (Dec. 31, 2008) (on file with Campbell Law Review). His listing included the following: (1) "I think there is a world market for maybe five computers." Thomas Watson, president of IBM 1943; (2) "Television won't be able to hold on to any market it captures after the first six months. People will soon get tired of staring at a plywood box every night." Darryl Zanuck, executive at 20th Century Fox, 1946; (3) "Nuclear-powered vacuum cleaners will probably be a reality within ten years." Alex Lewyt, president of Lewyt vacuum company, 1955; (4) "There is no reason anyone would want a computer in their home." Ken Olsen, founder of Digital Equipment Corporation, 1977; (5) "Almost all of the many predictions now being made about 1996 hinge on the Internet's continuing exponential growth. But I predict the Internet will soon go spectacularly supernova and in 1996 catastrophically collapse." Robert Metcalfe, founder of 3Com, 1995; (6) "Apple is already dead." Nathan Myhrvold, former Microsoft CTO, 1997; (7)""Two years from now, spam will be solved." Bill Gates, founder of Microsoft, 2004. *Id.*

Precisely because so many potential clients are likely to be interested in these concepts and possibilities on the front-end, it would stand lawyers in good stead to at least be able to converse intelligently on these topics. The reality is that the world of cryptotransactions, whether clients are interested in Coins, Tokens, Virtual Currencies, or ICOs, are incredibly complex, and clients will need sound legal advice. To provide that advice, attorneys will have to understand what clients are talking about. Only then can attorneys begin investigating and explaining the applicable regulations.

Without going into too much depth, here are the major regulations with which a lawyer may need to be familiar in order to speak intelligently about various aspects of Cryptocurrency regulation,[427] including: securities laws (both federal and state);[428] commodity trading regulations;[429] federal banking regulations—particularly relating to the Bank Secrecy Act[430] requirements concerning anti-money laundering (AML)[431] and know-your-customer (KYC)[432] requirements; money transmitter requirements (at both

427. For an extremely basic overview of these requirements, see Scott D. Hughes, *Cryptocurrency Regulations and Enforcement in the U.S.*, 45 W. ST. U. L. REV. 1, 2 (2017); *see also* James P. Brennan et al., *The Curious Case of Crypto*, 37 BANKING & FIN. SERVS. POL'Y REP. 8 (April 2018).

428. For a more thorough overview of federal securities laws as they apply to tokenized offerings, see Carol Goforth, *Securities Treatment of Tokenized Offeriings Under U.S. Law*, 46 PEPP. L. REV. (forthcoming 2019) (available in draft form at https://perma.cc/2M74-36QV).

429. For an article focusing on commodity regulations in this space, albeit focused on Bitcoin, see Mitchell Prentis, Note, *Digital Metal: Regulating Bitcoin As A Commodity*, 66 CASE W. RES. L. REV. 609 (2015). It is worth noting, however, that significant developments have occurred in the relatively short time since this article was published. *See* Stephanie A. Lemchuk, Comment, *Virtual* Whats?*: Defining Virtual Currencies in the Face of Conflicting Regulatory Guidances*, 15 CARDOZO PUB. L. POL'Y & ETHICS J. 319, 349 (2017) (advocating for the treatment of cryptoassets as commodities).

430. Bank Secrecy Act, 31 U.S.C. §§ 5311–32 (2012). As described by the Officer of the Comptroller of the Currency, the Bank Secrecy Act "establishes program, recordkeeping and reporting requirements for national banks, federal savings associations, federal branches and agencies of foreign banks." Office of the Comptroller of the Currency, *Bank Secrecy Act (BSA)*, U.S. DEPT. OF THE TREASURY, https://perma.cc/FH4Z-5VMD. Included in these requirements are various requirements concerning customer identification and other anti-money laundering efforts. *Id.*

431. For an explanation of AML requirements, see generally Stuart P. Lott & Blake B. Goodsell, *The "Fifth Pillar" of AML/BSA Compliance FinCEN Issues Final Rule for New Customer Due Diligence Requirements Under the Bank Secrecy Act*, BRADLEY (July 20, 2016), https://perma.cc/7RWX-45WR.

432. For an explanation of KYC requirements under the BSA, see generally Lowers & Associates, *Why KYC is the Backbone of BSA/AML Compliance*, RISK MGMT. BLOG (June 18, 2015), https://perma.cc/9RGH-7MRH.

the federal and state levels);[433] tax laws;[434] and in some states, specialized virtual currency business requirements.[435]

Cryptocurrencies and transactions involving them are subject to a number of different regulations, most of which probably cannot be understood absent at least a basic familiarity with the terms and concepts involved.[436] For example, the SEC has been particularly active in seeking to regulate transactions involving Cryptocurrency.[437] At one time, the SEC Chairman specifically opined that the he had not seen any ICO that did not involve the sale of a security.[438] The SEC has sent out dozens of subpoenas in support of its conclusion that most sales of Coins and Tokens involve the sale of securities[439] and require either registration or an exemption from the

---

433. *See generally* Sheng Zhou, Comment, *Bitcoin Laundromats for Dirty Money: The Bank Secrecy Act's (BSA) Inadequacies in Regulating and Enforcing Money Laundering Laws over Virtual Currencies and the Internet*, 3 J.L. & CYBER WARFARE 103 (2014); *see also* V. Gerard Comizio, *Virtual Currencies: Growing Regulatory Framework and Challenges in the Emerging Fintech Ecosystem*, 21 N.C. BANKING INST. 131 (2017).

434. For a discussion of various tax rules applicable to Cryptocurrencies see Sami Ahmed, *Cryptocurrency & Robots: How to Tax and Pay Tax on Them*, 69 S.C. L. REV. 697 (2018); Sarah-Jane Morin, *Tax Aspects of Cryptocurrency*, PRAC. TAX LAW. 56 (2018).

435. For example, the Uniform Regulation of Virtual Currency Businesses Act (described in some detail *supra* Section II.35) is designed to be implemented by individual states. Other states, such as New York and Wyoming, have already adopted laws relating to Cryptocurrencies. *See infra* notes 465–66.

436. For a listing of various regulatory responses being considered at the end of 2017, see Francine McKenna, *Here's How the U.S. and the World Regulate Bitcoin And Other Cryptocurrencies*, MARKETWATCH (Dec. 28, 2017 11:19 AM) (on file with Campbell Law Review).

437. The SEC recently released a joint statement with the Commodities Futures Trading Commissions (CFTC) specifically warning that they intend to be active in overseeing tokenized offerings regardless of the labels affixed to the interests being offered:

> When market participants engage in fraud under the guise of offering digital instruments—whether characterized as virtual currencies, coins, tokens, or the like—the SEC and the CFTC will look beyond form, examine the substance of the activity and prosecute violations of the federal securities and commodities laws. The Divisions of Enforcement for the SEC and CFTC will continue to address violations and bring actions to stop and prevent fraud in the offer and sale of digital instruments.

JD Alois, *SEC and CFTC Issue Joint Statement on Cryptocurrency Enforcement Actions*, CROWDFUND INSIDER (Jan. 19, 2018), https://perma.cc/GRF7-E778.

438. *See* Young, *supra* note 33.

439. *See, e.g.*, Bloomberg, *The SEC is Sending Subpoenas in Expanded ICO Crackdown*, FORTUNE (March 1, 2018), https://perma.cc/5TDK-USWR. "Over the last few months, the commission has asked for information from companies that have sold new virtual currencies to raise money for their projects, as well as advisory firms and lawyers who have helped with these sales, according to four people who have seen some of the subpoenas."

registration requirement in order to be legal.[440] The SEC has also strongly asserted its right to protect investors against fraud in these kinds of transactions.[441]

With that in mind, think about what a lawyer would need to know in order to consult with a client who wants to talk about ICOs, even in a very preliminary fashion. The attorney would obviously need to know what an ICO is before he or she could begin offering advice about the SEC's position about how such deals are to be treated and why.[442] Without understanding that an ICO is radically different from an IPO, even an experienced securities lawyer might fail to appreciate why most ICOs worldwide have simply excluded US-based investors from Token-based crowd-funding.[443] Similarly, it would be hard to explain why, within the U.S., ICOs appear to have transitioned from public to private or limited offerings.[444] Moreover, if a client wants to pursue an international offering of Coins or Tokens, the attorney must know that the international regulation of ICOs is even more complex because nations take radically different approaches to tokenized offerings.[445] For example, the Chinese government recently attempted to ban ICOs outright.[446] The Philippines, where Cryptocurrencies have been extremely popular, also plans to regulate ICOs.[447] At the other end of the spectrum, the Venezuelan

---

Nathaniel Popper, *Subpoenas Signal S.E.C. Crackdown on Initial Coin Offerings*, N.Y. TIMES (Feb. 28, 2018) (on file with Campbell Law Review).

440. The requirement that "securities" be registered before they are offered or sold appears in section 5 of the Securities Act of 1933. Securities Act of 1933, 15 U.S.C. § 77e. Exemptions from the registration requirement are in sections 3 and 4. 15 U.S.C. §§ 77c & 77d; *see also supra* note 346.

441. *See* Alois, *supra* note 437.

442. *See* Young, *supra* note 33 (describing SEC Chairman Jay Clayton's general understanding that most ICOs (in fact all of them, so far) are securities). For a technical statement of the SEC position, see *Statement on Cryptocurrencies and Initial Coin Offerings*, U.S. SEC. & EXCH. COMM'N, https://perma.cc/VS37-B475.

443. Young, *supra* note 33.

444. *Id.*

445. International regulation of Cryptotransactions in general is incredibly complicated. For an overview of some of the varied international regulatory approaches, see Karsten Wöckener et al., *Regulation of Initial Coin Offerings*, WHITE & CASE (Dec. 15, 2017), https://perma.cc/ZQ49-2H77. For a longer list of international reactions, see McKenna, *supra* note 436.

446. Marr, *supra* note 53.

447. Sujha Sundararajan, *Philippines SEC Plans to Regulate Cryptocurrencies, ICOs*, COINDESK (Jan. 29, 2018), https://perma.cc/AZZ8-WVVJ. ("The Philippines' Securities and Exchange Commission said on Monday it is crafting rules to regulate cryptocurrency transactions to protect investors and reduce the risk of fraud. The regulation, which will

government has launched a Token of its own.[448] Researching this kind of issue would be virtually impossible without an understanding of the basic terminology involved in ICOs.

Suppose the client is not one that can be trusted to be completely candid with potential purchasers about the potential limitations or risks associated with a proposed Coin or Token. In that case, not only the SEC but also the Commodity Futures Trading Commission (CFTC) will need to be considered. The CFTC has actively sought to regulate misleading Coin and Token sales by first classifying Bitcoin as a commodity in 2015.[449] Although its initial ruling was originally limited to Bitcoin, the CFTC has clearly asserted that it has broader jurisdiction.[450] More recently, the CFTC appears to have been simultaneously insisting that it does not want to overregulate[451] while also actively working to police fraud in connection with the purchase and sale of Cryptocurrencies.[452] Without understanding

---

cover issuance and registration of cryptocurrencies, is expected to be finalized this year . . . .").

448. Daniel Palmer, *Venezuela's 'Petro' Token Launches in Pre-Sale*, COINDESK (Feb. 20, 2018), https://perma.cc/P9V7-K4R7 (stating that "pre-sale" refers to the period of time in which subscriptions for ultimate purchases are solicited and accepted).

449. *CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps Without Registering*, U.S. COMMODITY FUTURES TRADING COMM'N, (Sept. 17, 2015), https://perma.cc/8KT9-ZDHX. The approach was initially applied only to Bitcoins, and the CFTC has recently announced a desire to avoid stifling innovation and efficiency. *See CFTC Plans to Take "Do No Harm" Approach to Crypto Regulation*, RODMAN LAW GROUP, LLC (Feb. 7, 2018), https://perma.cc/DS7N-CVR7.

450. While the CFTC was originally cautious in deciding what Cryptocurrencies to claim as being within its sphere, that has now changed, and it is willing to go to court in order to assert its authority. In March of 2018 the District Court in the Eastern District of New York agreed with the CFTC's contention in Commodity Futures Trading Comm'n v. McDonnell, 287 F. Supp. 3d 213 (E.D.N.Y. 2018), that the CFTC had concurrent jurisdiction over virtual currencies. "The jurisdictional authority of CFTC to regulate virtual currencies as commodities does not preclude other agencies from exercising their regulatory power when virtual currencies function differently than derivative commodities." *Id.* at 228.

451. In testimony to the Senate Committee on Banking, Housing and Urban Affairs on February 6, 2018, Chairman Giancarlo explained that "[i]t strikes me that we owe it to this new generation to respect their enthusiasm about virtual currencies with a thoughtful and balanced response, not a dismissive one." Michael Pearl, *Giancarlo 2020? Crypto World Has a New Hero—the Head of the CFTC*, FINANCE MAGNATES (July 2, 2018), https://perma.cc/4RFB-Z8F6.

452. As one source noted, "it is clear that both the SEC and CFTC are picking up steam in their efforts to command a presence in the fast-developing world of virtual currencies." King & Spalding, *Dividing Up the Sandbox: Recent Actions and Public Statements Demonstrate How the SEC and CFTC Are Dividing up the Cryptocurrency and Crypto-Token Enforcement Landscape*, JDSUPRA (Feb. 8, 2018), https://perma.cc/DB9G-K9VW.

what Cryptocurrencies such as Bitcoin are, an attorney is limited in his or her ability to convey information about the rationale behind this approach or to understand how recent actions of the CFTC cast doubt on the once-popular notion that the CFTC is taking a hands-off approach.[453]

Similarly, the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") has issued guidance which requires certain intermediaries in Cryptocurrency transactions to register as "money service businesses."[454] This would apply whenever a client wants advice about whether to accept and convert or exchange Cryptocurrencies, particularly if large amounts are involved. An attorney must understand how a client's Cryptocurrency or proposed business idea will function in order to offer advice about whether these rules apply. The consequences for not understanding these rules can be severe.[455] For example, in at least one instance, the Department of Homeland Security seized assets owned by a Bitcoin Exchange on the grounds that the owner was involved in currency transfers that were not appropriately registered with FinCEN.[456] In another example of how the BSA requirements apply to Cryptocurrencies, Ripple was forced to pay a large fine for failing to comply with various BSA requirements.[457]

The I.R.S. also has rules affecting Cryptocurrency transactions, including a determination that Cryptocurrencies are property and not

453. Some of the CFTC's actions, which appear to be aimed at stopping fraudulent transactions, are fully comprehensible, although the basis for CFTC involvement may not be immediately obvious when there is no swap or contract for future delivery. For a discussion of one of the CFTC's most recent actions, see Keith Miller et al., *supra* note 329.

454. U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, FIN-2013-G001, *supra* note 21 (clarifying the coverage of regulations that implement the federal Bank Secrecy Act to persons engaged, among other things, in the receipt, distribution, exchange, and transmittal of virtual currencies).

455. Fines for non-compliance with FinCEN requirements can run into the hundreds of thousands or even hundreds of millions of dollars. For example, Ripple was fined a comparatively small $700,000. *FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger,* U.S. DEP'T TREASURY FIN. CRIMES ENF'T NETWORK (May 5, 2015), https://perma.cc/9T2V-9GJP. At the other end of the spectrum, BTC-e was fined $110 million. *FinCEN*, *supra* note 8.

456. Joe Mullin, *Feds Seize Money from Dwolla Account Belonging to Top Bitcoin Exchange Mt. Gox*, ARS TECHNICA (May 14, 2013), https://perma.cc/Z82L-DDW4. For additional discussion about this intervention, see Stephen T. Middlebrook & Sarah Jane Hughes, *Virtual Uncertainty: Developments in the Law of Electronic Payments and Financial Services*, 69 BUS. LAW. 263, 264 (2013).

457. In 2015, the Financial Crimes Enforcement Network (FinCEN) reached a settlement with Ripple pursuant to which Ripple paid a $700,000 fine. Van Valkenburgh, *supra* note 340.

currency;[458] this could be relevant in all of the scenarios mentioned in the preceding paragraphs. In order to understand the ramifications of the I.R.S. position, it is certainly necessary to understand that "Cryptocurrency" is not limited to Coins or Tokens that are actually intended to serve as a replacement for conventional currencies. In addition, knowing that Coins and Tokens can both fit within existing definitions of "Virtual Currency" is essential for even basic tax research in this area.

While the SEC, CFTC, FinCEN (which acts to enforce the BSA),[459] and the I.R.S. may be the most visible federal agencies, they are not the only ones interested in Cryptocurrencies. In response to calls for greater involvement,[460] the Consumer Financial Protection Bureau has issued

458. *I.R.S. Notice, supra* note 309 ("For federal tax purposes, virtual currency is treated as property."). The I.R.S.'s designation of Cryptocurrencies as "property" instead of as "currency" deprives the trader/user of favorable tax treatment afforded to foreign currency transactions and forces the taxpayer to track his or her "basis" in each unit of currency upon the sale or exchange and to calculate any net gain or loss realized. *Id.*

459. FinCEN is a bureau within the U.S. Department of the Treasury, and according to the Treasury Department, its mission is to "[s]afeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities." *Congressional Budget Justification and Annual Performance Report and Plan 3*, U.S. DEP'T TREASURY FIN. CRIMES ENF'T NETWORK (2019). This obviously gives FinCEN authority over the Bank Secrecy Act's anti-money laundering (AML) and Know-your-customer (KYC) requirements. Robert E. Braun, *The U.S. Treasury Wants to Know Your Customers, No Matter What the Currency,* LEXOLOGY (Apr. 23, 2018), https://perma.cc/8EPS-FTTC; *see also supra* notes 327 & 417–19 for a discussion of these requirements.

FinCEN receives about 1,500 Suspicious Activity reports relating to Cryptocurrencies each month. *Helen, The US Department of the Treasury is Developing an Information Sharing Platform for Crypto Exchanges*, COINSTELEGRAM (Aug. 13, 2018), https://perma.cc/9QJX-RHXE. It is therefore not surprising that the bureau is active in seeking effective oversight of Cryptocurrencies. This includes regulation of issuers and persons who assist in the exchange of Cryptocurrencies. *See, e.g., FinCEN, supra* note 8. FinCEN also has jurisdiction when the activity involves potentially illicit money transmitter activities.

For example, in the Ripple case discussed *supra* note 457, FinCEN suggested that when an issuer sells a token (XRP in the Ripple case) in a transaction that involves money transmission, it requires the issuer to register with FinCEN and comply with its regulations. Van Valkenburgh, *supra* note 340. Failure to comply with those requirements can result in monetary penalties and potentially jail time for management or other control persons. *Id.*; *see also* Borchgrevink, *supra* note 338, for an additional consideration of FinCEN's role in money transmitter regulation.

460. "On June 26, 2014, the Government Accountability Office released a report responding to a request from Senator Tom Carper, Chair, Senate Committee on Homeland Security and Governmental Affairs. That report called for, among other things, more involvement by the Consumer Financial Protection Bureau." *Advancing, supra* note 63, at 510.

consumer alerts and has proposed clarifying regulations to account for Virtual Currencies.[461] Learning about and understanding any such regulations will also require a familiarity with the terms and concepts.

In addition, at the state level, both the Conference of State Bank Supervisors[462] and the Uniform Law Commission[463] have created new projects aimed at Cryptocurrency regulation, and the North American Securities Administrators Association is considering the issue.[464] Individual states are not waiting for uniform regulation, with states like New York adopting regulations requiring Virtual Current participants to acquire a "BitLicense."[465] At the other end of the spectrum, some states have taken very pro-crypto positions,[466] but understanding what those regulations actually mean for any client will certainly require being able to talk intelligently about the interests and concepts behind Coins, Tokens, or other Blockchain projects.

This article barely scratches the surface of the knowledge needed to provide competent legal advice in these arenas. Hopefully, however, it provides a starting point for intelligent conversation with clients who need legal advice involving these concepts.

---

461. Consumer Fin. Prot. Bureau, *Risks to Consumer Posed by Virtual Currencies*, CONSUMER ADVISORY (Aug. 2014), https://perma.cc/6PFA-L6DJ. As for proposals considering how CFPB rules might apply to virtual currencies, see Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z), Fed. Reg. 77102, 77121 (Dec. 23, 2014) (to be codified at 12 C.F.R. §§ 1005 & 1026) (noting that CFPB's review of virtual currencies and related products is "ongoing").

462. The Conference of State Bank Examiners ("CSBS") issued a model regulatory framework for Virtual Currencies on September 15, 2015. CONFERENCE OF STATE BANK SUPERVISORS, *supra* note 404. The policy document is based on the CSBS conclusion that "activities involving third party control of virtual currency, including for the purposes of transmitting, exchanging, holding, or otherwise controlling virtual currency, should be subject to state licensure and supervision." *Model Regulatory Framework for Virtual Currencies*, CONF. ST. BANK SUPERVISORS (Mar. 30, 2017), https://perma.cc/2M53-5YMM.

463. For a description of the ULC's work on the Uniform Act, and the contents of that Act, see *supra* Section II.35 (describing the Uniform Act as promulgated by the ULC in October of 2017).

464. In May 2018, the North American Securities Administrators Associations (NASAA) announced a coordinated effort to investigate fraudulent Cryptocurrency sales and ICOs, as well as enforcing other regulatory requirements. *State and Provincial Securities Regulators Conduct Coordinated International Crypto Crackdown*, N. Am. Sec. Administrators Assoc. (May 21, 2018), https://perma.cc/M9MJ-PPVY.

465. *See* N.Y. FIN. SERV. LAW § 200 (2017).

466. H.B. 0070, 64th Leg. (Wyo. 2018); *see also* Shipkevich, *supra* note 338 (discussing briefly the current state of Wyoming law governing Cryptocurrencies).