A Cryptocurrency Orientation for Property Insurance Professionals

By Joseph Lavoie

Joseph R. Lavoie *is an associate attorney at Sulloway & Hollis, PLLC, in Concord, New Hampshire, where his practice focuses on insurance coverage matters and general litigation. He has given presentations to lawyers, insurance industry professionals, and college students on various cryptocurrency issues. Lavoie may be reached at jlavoie@Sulloway.com.*

> *Buildings burn down the same way they burned down since the 1700's. . . . Any building has a one percent chance of burning down. I have no clue what the chance of cyber threats is to your keys. It's just a different animal, and insurance has difficulty adapting to these new e-commerce kind of risks.*
> —Brent Elstrom[1]

Open any news source today, and there is a good chance that you will find an article on cryptocurrency. Bitcoin, which emerged over a decade ago, is now a household name. While the space is still relatively small, it continues to grow both in overall value and in user base. Importantly, insureds are beginning to claim Bitcoin losses on policies that predate cryptocurrency.[2]

This article serves as an orientation guide for professionals in the property insurance industry examining cryptocurrency for the first time. First, the article traces the history of Bitcoin because the ideas that bore Bitcoin attracted the early adopters and have shaped the entire space. Second, the basics of cryptocurrency are presented. Next, the article provides an introduction to the cryptocurrency ecosystem, explaining how transactions are made on a blockchain and how coins are stored. Then, there is a brief discussion on crime and some relevant government regulations. Lastly, the article highlights issues about which property insurance professionals should be aware as they enter the cryptocurrency space.

This article represents a current description of an emergent technology. Readers should be aware that in the rapidly developing cryptocurrency industry, new advances and practices could render parts of this article incorrect and outdated at any time.

Cryptocurrency: A History

Cryptocurrency can be traced to a small gathering of cryptographers, programmers, and entrepreneurs who met back in 1992 to discuss their shared interest in computer science, mathematics, and privacy.[3] The group met regularly until it outgrew the original meeting space and became a mailing list that eventually included hundreds of people.[4] The participants of the mailing list became known as the Cypherpunks.[5] Interested in the concepts of privacy and freedom, the Cypherpunks gave rise to early attempts at creating a digital currency that did not rely on a centralized authority to legitimize and regulate transactions.[6]

The double-spend problem. The most notable attempts were B-Money, Bitgold, and Hashcash—which, despite their Midas-like monikers, failed to develop or monetize.[7] The reason that B-Money, Bitgold, and Hashcash are not in the news today is because they failed to resolve major problems inherent in implementing a digital currency. One of the greatest hurdles was the double-spend problem.

Double-spending refers to the act of spending a unit of currency more than once.[8] For example, a fraudster gives a unit of currency to John. Then, the fraudster gives the same unit of currency to Andrew. This is not a problem for physical currency. Once the fraudster hands a dollar to John, the fraudster is no longer in possession of the dollar and is unable to hand it to Andrew. The concept of possession is murkier for digital coins. Possession of a digital coin is merely the ability to access the coin and to exclude others from accessing the coin. All that is being accessed is a string of code, and that code is susceptible to manipulation.[9]

Pre-Bitcoin, there was no scalable mechanism to prevent a digital coin from being spent twice.[10] Moreover, neither Andrew nor John had any means to verify whether he was receiving a valid coin.[11]

Satoshi Nakamoto. In traditional systems of handling digital assets, the double-spend problem is eradicated by reliance on a centralized authority to authenticate transactions. However, digital currencies without a centralized authority need a protocol to prevent double-spending. This was one of the problems with which the Cypherpunks grappled in their early attempts, but there was no scalable solution until Satoshi Nakamoto published his Bitcoin white paper.

In October 2008, Nakamoto, a newcomer to the Cypherpunk mailing list, circulated a white paper to the list titled *Bitcoin: A Peer-to-Peer Electronic Cash System*, which proposed an electronic payment system called *Bitcoin*.[12] Bitcoin addressed the double-spend problem through absolute transparency: "[t]he only way to confirm the absence of a [previous] transaction is to be aware of all transactions."[13]

Cryptocurrency: The Basics

Blockchain 101. Nakamoto's white paper presented Bitcoin as a digital currency hosted on a "blockchain."[14] A blockchain is simply a means of storing information.[15] In industry terms, *blockchain* means a digital distributed ledger system that records transactions and other information in chronological order.[16] A blockchain is digital because there is no tangible form of a blockchain. The term *distributed ledger system* requires a bit more to unpack.

It is helpful to start with the common understanding of the term *ledger*. A ledger is an accounting. For our purposes, picture Scrooge in a top hat hunched over a leather-bound book scratching figures with a feather quill; the book is the ledger. Picture the ledger being copied to back up the content therein. If there is a conflict between a copy and the original, it is likely that the original will be regarded as the most accurate.

In stark contrast to the ledger under the arm of Scrooge, a blockchain distributed ledger system is a network of ledgers with equivalent authority maintained by consensus.[17] Instead of a recording system with an original ledger, a distributed ledger system is a recording system in which information is entered on all ledgers contemporaneously.[18] If there is a conflict between ledgers, the information reflected in the majority of the ledgers controls. As long as the majority of the ledgers contain accurate information, the network retains its integrity.[19]

There are several characteristics that most, if not all, blockchains have in common. In any network purporting to be a blockchain, information is stored chronologically on "blocks."[20] A block is a representation that illustrates how information is segmented and organized chronologically—a chain of information segments could have been appropriately termed *trianglechain*.

The term *chain* in *blockchain* refers to the connection between each block. Unlike a traditional ledger, where each line contains independent information, each new block in a

blockchain contains data from previous blocks. This is accomplished by the inclusion of a string of alphanumeric characters that reflect and represent information contained in the prior block.[21] This string of characters is referred to as a timestamp or a hashstamp.[22] Because each block contains a hashstamp reflecting the previous block, the newest block necessarily reflects information from the first block, or *genesis block*.[23] Thus, a series of chronologically organized blocks of information that are linked inherently to previous blocks becomes a blockchain.

Hashstamp. The hashstamp feature is one of the characteristics of blockchain that lends itself to network integrity. With a traditional ledger, a bad actor with an eraser can alter an entry on page two of the ledger without altering information on page five. With a blockchain, a bad actor can alter transactional information on a block from an earlier date, but every subsequent block's hashstamp will change to reflect the amended data. In this situation, the ledger with the altered information conflicts with all of the other ledgers in the network. Under a distributed ledger system, there can be hundreds of ledger hosts. When hundreds of ledgers contain identical hashstamps and one ledger deviates, locating the fraudulent activity is a minimal burden. In sum, transparency prevents successful fraud.

Mining. "Mining is the process by which transactions are verified and added to the public ledger."[24] Mining is, essentially, the proof-of-work protocol.[25] *Miner* is a term that refers to individuals and entities that use their computers or hardware systems to complete "computationally difficult puzzles that appear at the end of each Block when it is added to the 'chain.'"[26] When a miner completes a puzzle, four things occur: (1) the current block closes, preventing new information from entering; (2) a new block is formed as next in line on the chain; (3) new information begins to be recorded in the new block; and (3) the front-running miner receives Bitcoin as a prize for completing the puzzle.[27] Thus, blockchains have motivated individuals who verify the integrity of the system and are rewarded with cryptocurrency.

Mining does have its own complications that will need to be addressed in the coming years. People and companies can pool computer equipment together to create mining pools (i.e., warehouses full of machines running at full speed). This increases the risk of, as described below, a coordinated 51 percent attack.

Attack of the majority. A system built on mining is susceptible to a majority or 51 percent attack. A 51 percent attack is a hypothetical, concerted effort by a blockchain's majority to manipulate data on that blockchain.[28]

There is an important nuance here. A 51 percent attack is not an attack by the majority of users on a blockchain. Rather, it is an attack by the people and entities controlling at least 51 percent of the resources or mining power on a blockchain. Hypothetically, a single mining pool controlled by a large entity like a corporation or government could take control of a blockchain. This is, however, very unlikely for a number of reasons, but they are beyond the scope of a cryptocurrency orientation paper.

Cryptocurrency characteristics. There are certain characteristics that most, if not all, cryptocurrencies share.[29] A cryptocurrency is a currency-like digital interest.[30] Cryptocurrencies are independent of a central authority and "operate on a peer-to-peer basis."[31] These peer-to-peer networks use cryptography to eliminate the need for a centralized, trusted authority.[32] A cryptocurrency transaction is nonreversible. This cannot be overstated. The "send" button is a permanent action. Even mistaken or fraudulent transactions cannot be reversed.

The Blockchain Ecosystem

This section provides a general outline of the cryptocurrency ecosystem. This is in no way an exhaustive description, but it does describe the major components in the space.

Public versus private blockchains. There are two main types of blockchains today: public and private.[33] A public blockchain, such as Bitcoin, allows anyone to enter the network as a miner or user.[34] In contrast, a private blockchain permits only predetermined or select individuals or entities to act as ledger hosts and users.[35] The latter is more appropriate for entities putting sensitive information on a blockchain or for closed systems.

Forking and new blockchains. As discussed above, blockchains are networks of consensus. Individuals and entities that embody the blockchain can agree to change protocols or to include updates to the system as they see fit.[36] When this occurs, the blockchain is said to "fork." In some instances, users agree to migrate to a new and upgraded blockchain.[37] This is known as a *hard fork*.[38] When some holdout users refuse to leave, a blockchain network can fracture into two distinct blockchains.[39]

Smart contracts. A "smart contract" is a self-executing contract recorded in code on a blockchain.[40] Smart contracts are agreements reduced to code so that when a condition is satisfied, performance is automatically triggered.[41]

To date, smart contracts are best suited for if-then agreements.[42] For example, Vitalik sells John a house. When John receives the deed to the home, the code triggers the automatic transfer of Bitcoin to Vitalik's wallet. There is no need for escrow.

There is no consensus regarding the legal status of a smart contract. Some academics dispute whether a smart contract is legally enforceable.[43] In fact, any "automatic contract" or "self-executing contract" is problematic. Here, an illustration helps. Picture a vending machine. Put a dollar into a vending machine, and the internal workings of the machine produce a soda. The pressing of the button is the agreement. The internal workings of the machine are performance. One could argue that the agreement to create a smart contract is the contract, while the self-executing code is like the internal workings of a vending machine. This issue has not been tested in courts.

Another issue involving smart contracts is the issue of how triggering information is input into a smart contract and, perhaps more importantly, who is authorized to input such information into the smart contract. This requires a trusted party, which is exactly what cryptocurrency was created to avoid. The problem of needing a party to input information into a smart contract to trigger performance is known as the oracle problem. *Oracle* refers to the trusted party that inputs data onto a blockchain.[44] One blockchain project called *Augur* is attempting to become an oracle, but its efficacy and integrity are yet to be proven.[45]

Coins versus tokens. There is a distinction between cryptocurrencies as coins and cryptocurrencies as tokens.[46] Cryptocurrencies as coins function as a medium of exchange. In contrast, a token facilitates a program. If the program were a car, then tokens are the fuel. For example, *Golem* is a program built on a blockchain that allows users to remotely "loan" idle computer-processing power to others.[47] For those seeking to rent processing power, they need to spend *Golem* tokens.

For the purposes of a cryptocurrency orientation, it is important to remember the different goals of a token and a coin. Cryptocurrency coin developers strive to increase the coin's utility as a medium of exchange: transaction speeds, integrity of the network, security, stability, increased acceptance by merchants. A cryptocurrency token developer also may be concerned with such goals, but these developers are creating a program that has a functionality apart from the token's

utility as a medium of exchange.[48] This means that the valuation of a cryptocurrency-as-coin blockchain is different from that of a cryptocurrency-as-token blockchain.

Exchanges. So, where can the average person buy Bitcoin?[49] Cryptocurrency can be purchased at a cryptocurrency "exchange."[50] Exchanges are websites accessible on your browser where users can purchase and trade cryptocurrencies.[51]

There are many exchanges with varying degrees of credibility. More reputable exchanges comply with know-your-customer laws, while others emphasize anonymity. Some exchanges permit wire transfers from banks, which is typically the first step for first-time buyers: send money to the exchange, use that money to purchase cryptocurrency, and then trade cryptocurrencies.

Wallets. Cryptocurrency owners store their coins and tokens in digital wallets.[52] A cryptocurrency wallet acts like a post office box. There is a public address that everyone can see, but only the wallet owner can access the wallet by use of a private key.[53] A wallet owner needs the private key to send cryptocurrency from her wallet to another address.[54] While this heightened security is useful, it also can be problematic. Because there is no central authority on a blockchain, a user who forgets her key or forgets how to access the key will have no means of accessing cryptocurrency stored in the wallet. The coins in that wallet effectively become frozen.

There are two types of wallets: hot and cold. A hot wallet is one that is hosted online.[55] These are accessed through a web browser or hosted on an exchange. A cold wallet is a device that stores passcodes and enables wallet owners to access their accounts without physically entering a passcode.[56] The functionality of a cold wallet is like that of an external hard drive or thumb drive: a cold wallet can be plugged into your computer when in use and removed when no longer in use.

The benefit of a cold wallet is added protection of the private key. Hot wallets require users to enter the private key on their devices, computer or mobile, which are always susceptible to remote key tracking and screen mirroring. Cold wallets may eliminate the need to ever type a private key by loading the private key onto the cold wallet device. The user just needs to plug the cold wallet device into a computer and the wallet opens.

Custodial wallets. A custodial wallet is an exchange's wallet; such wallets are both extremely useful and extremely problematic. When a user utilizes a wallet hosted on an exchange, that user trusts the exchange to have the cryptocurrency it promises to be storing.

Last year, the founder of cryptocurrency exchange Quadriga CX tragically died at age 30.[57] As the owner of an exchange, he was responsible for the cryptocurrency that his users entrusted to the exchange. In fact, he was storing $190 million worth of cryptocurrency when he died.[58] The founder did not create a means for anyone else to learn of his private key, and so the $190 million worth of cryptocurrency remains inaccessible.[59]

Beyond Bitcoin. While Nakamoto may have intended blockchain as a means of implementing and scaling a digital currency, blockchain now is being applied to a variety of industries and with applications beyond a medium of exchange.[60] Blockchain's application to supply-chain systems is the most intuitive.[61] Already, blockchain has been implemented on supply chains to improve authentication of inventory and proof of provenances, where tracing the geographic source of products is important.[62] One source estimates that worldwide there is $3.7 trillion lost each year due to deliberate supply-chain fraud.[63]

Crime and Government Regulation

For many, cryptocurrency is synonymous with crime. Cryptocurrency is used to facilitate crime, and those in the cryptocurrency space are frequently the victims of crime.

Some cryptocurrencies even add features to their blockchain to increase user privacy, which makes it more difficult for law enforcement to track illegal activity.[64] Monero is one such example; it uses protocols to obfuscate transactional information recorded on its blockchain.[65] Another cryptocurrency, Zcash, effectively erases transactional data through zero-proof technology after a transaction is complete.[66] For the motivated bad actor, these privacy-focused cryptocurrencies can be used on top of the Onion Router, which allows its users to anonymize their IP addresses to remain further in the dark.[67]

However, it is becoming apparent that cryptocurrency is not ideal for criminal enterprise. Anonymous cryptocurrency transactions, where all one needs is a private key, might be attractive to criminals seeking to avoid law enforcement, but cryptocurrency offers anonymity only as long as someone is not looking.[68] Every transaction on a blockchain is recorded and transparent.[69] This is not conducive to illegal acts. If a bad actor wants to make a $1 million bribe and sends $1 million worth of Bitcoin to wallet X for that purpose, law enforcement just needs to monitor wallet X and trace the Bitcoin. And, unfortunately for criminals, law enforcement need not be in a hurry to perfect its ability to track illegal transactions on blockchains because those transactions are permanently stored on the network's ledgers.

IRS responds. In response to the popularity and notoriety of cryptocurrency, the Internal Revenue Service (IRS) published Notice 2014-21 to clarify its stance on virtual currencies.[70] The IRS determined that virtual currencies—a category under which cryptocurrencies fall—are to be treated as property.[71] This means that general tax principles that apply to property also apply to cryptocurrency.

For purposes of calculating income, the IRS values cryptocurrency at the time it is received and by its fair market value.[72] A mined virtual currency is gross income valued at the fair market value as of the date of receipt.[73] Wages paid in cryptocurrency are also taxable.[74]

SEC responds. The U.S. Securities and Exchange Commission (SEC) also has turned its regulatory attention to cryptocurrency.[75] The SEC has focused on initial coin offerings (ICOs), which are akin to initial public offerings.[76] An ICO allows a company to raise money through the sale of unmined tokens or coins.[77] It is estimated that in 2017 ICOs raised over $6 billion.[78] Historically, ICOs have been used to fund projects very early on in their development. After many investors lost their investments to fraud and incompetence, the SEC entered the scene.[79]

SEC regulation is beyond this cryptocurrency orientation, but the insurance industry should recognize that not every ICO falls under the SEC's jurisdiction. Recently, the SEC issued its first no-action letter to a company seeking to raise funds through an ICO.[80] The SEC issued the letter with the appropriate barrage of "this is guidance only" language and then provided guidance for companies still wishing to use ICOs to raise funds. The SEC's letter lists the reasons for the no-action letter:[81]

- The company does not intend to use the funds received from sales of the tokens to finance the development of the blockchain; instead, the blockchain will be fully operational at the time of the sale.
- The tokens will be usable and functional at the time of the sale.
- The tokens can only be transferred to and stored at the private blockchain's wallets.
- Each token will be sold for and will represent the value of one U.S. dollar.
- The company issuing the tokens will repurchase tokens for one U.S. dollar each.

- The tokens will be marketed to show their functionality as opposed to their potential for increase in value.

Insurance Overview

This section gives a brief history of cryptocurrency insurance, details the litigation activity that has occurred, highlights a few concerns for the property insurance industry, and discusses how blockchain technology may be incorporated into the administration of insurance.

Brief history of cryptocurrency insurance. In 2014, Great American Insurance Company began offering Bitcoin insurance coverage to businesses: policy endorsements covering criminal acts expressly addressed Bitcoin.[82] One year later, the Bitcoin Insurance Agency became

> the first insurance and financial services company specifically created to handle the insurance needs, from the routine to the unique, of companies in the bitcoin [*sic*] industry. Since then insurers such as CHUBB, Mitsui Sumitomo Insurance, and XL Caitlin have entered the space with new products. More insurers are on the way.[83]

Lloyd's of London published the following list in 2015, which highlights specific Bitcoin and cryptocurrency risk factors:[84]

1. Flawed key generation: a mistake that allows hackers to decrypt private keys
2. Transaction malleability: tricking consumers into sending a payment multiple times
3. Fifty-one percent attack: a mass computing attack to overpower an entire blockchain
4. Sybil attacks: surrounding one network node with malicious ones to manipulate it
5. DDoS attacks: shutting down a network by bombarding it with fake requests
6. Consensus of fork risk: splitting of one currency into two

Lloyd's of London also published the following list of best practices for digital currencies:[85]

1. Server-side security: utilizing industry techniques or outsourcing to the cloud
2. Cold storage: storing private keys that access crypto assets off-line (preventing hacks)
3. Multi-signature and control person: distributing transaction authority to multiple individuals
4. Hybrid wallets: not storing private keys on an institutional level

Cryptocurrency and litigation activity. To date, there is only one major published property insurance coverage decision, and the litigation is still ongoing. The case, *Kimmelman v. Wayne Insurance Group*,[86] is a declaratory judgment action in which the insured is claiming $16,000 worth of Bitcoin on a homeowners policy issued by Wayne Insurance Group. The insured claims that his Bitcoin was stolen. Wayne Insurance responded by covering the loss as "money" with a $200 cap. The insured brought a bad-faith action against Wayne Insurance, and Wayne Insurance moved for judgment on the pleadings.

The trial court denied Wayne Insurance's motion after finding that Bitcoin was not money. The trial court surveyed the United States for any authority as to whether Bitcoin was

money or property. The court could cite only IRS Notice 2014-21. Consistent with Notice 2014-21, the court found that Bitcoin was property and denied the insurer's motion.

Insurance concerns. "Because Bitcoin hasn't been around long, insurers lack the history to draw a risk analysis."[87] The cryptocurrency space is still relatively small. There are relatively few users, and the risk pool is minimal. Even more troublesome, the people attracted to cryptocurrency may not be eager to share the personal information necessary to accurately access the risks involved.

The following are some general areas of concern:

- *Volatility*. Extreme volatility remains a hurdle to insuring cryptocurrency. The following illustrates the problem that this poses: In 2010, a computer programmer purchased two pizzas with 10,000 Bitcoins.[88] At that time, the parties valued Bitcoin at .003 cents.[89] Due to the increasing value of Bitcoin, if that same programmer decided to spend 10,000 Bitcoins for pizza in 2013, he could have purchased $65,000 worth of pizza.[90] In late 2017, he might have purchased $2 million worth of pizza.[91]

- *Traditional policies*. Insureds may try to cover cryptocurrency losses with traditional forms, but gaps and exclusions will leave many without coverage.[92] New agencies, like Bitcoin Financial Group, LLC, are emerging as specialists in the field.[93]

- *Fraud*. The nature of cryptocurrencies and blockchain technology will make it difficult to determine if insureds are making claims for losses that they initiated.[94]

- *Valuation*. The valuation of cryptocurrency is a novel issue that each jurisdiction will have to address. Though the IRS's valuation at time of receipt and according to fair market value may influence this analysis, this issue is by no means resolved.

In the future, insurance carriers may need to require as conditions to coverage that users maintain wallets in specific exchanges or that cold wallets are stored in traditional banks.

Application of blockchain to insurance. While blockchain is poised to affect a number of industries, insurance is near the top of that list.[95] Specifically, smart contracts could have a positive impact on the insurance industry. Smart contracts have a direct application to if-then insuring agreements: if this discrete event occurs, then the company shall pay X.[96] Coverage afforded through a parametric insuring agreement could be combined with blockchain technology to reduce the time it takes insureds to rebuild their businesses, homes, and lives.[97]

Conclusion

Cryptocurrency can seem a strange and foreign technology. Not only is it riddled with jargon, but there is no consensus on the jargon. This can make learning about cryptocurrency a challenge. This orientation is an attempt to provide cryptocurrency and blockchain basics at a high level for the property insurance industry.

Notes

1. Eleonora di Liscia, *The Emerging Cryptocurrency Coverage Market*, NEW APPLEMAN ON INSURANCE: CURRENT CRITICAL ISSUES IN INSURANCE LAW, at IV (Winter 2018).
2. Kimmelman v. Wayne Ins. Grp., 2018 Ohio Misc. LEXIS 1953 (2018).

3. PetriB, *The Untold History of Bitcoin: Enter the Cypherpunks*, MEDIUM (Jan. 26, 2018), https://medium.com/swlh/the-untold-history-of-bitcoin-enter-the-cypherpunks-f764dee962a; Reuben Yap, Op-Ed, *Cypherpunk Essentials: A Beginner's Guide to Crypto Privacy*, NEWS.BITCOIN (Oct. 17, 2018) https://news.bitcoin.com/cypherpunk-essentials-a-beginners-guide-to-crypto-privacy.
4. *Id.*
5. *Id.*
6. *Id.*
7. *Id.*
8. Bisade Asolo, *Double-Spending Explained*, MYCRYPTOPEDIA (Dec. 21, 2018) www.mycryptopedia.com/double-spending-explained.
9. *Id.*
10. *Id.*
11. *Id.*
12. SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (2008), https://bitcoin.org/bitcoin.pdf; *see also* Adam J. Kolber, *Not-So-Smart Blockchain Contracts and Artificial Responsibility*, STAN. TECH. L. REV. 198, 206 (2018).
13. NAKAMOTO, *supra* note 12, at 2.
14. *Id.*
15. *Id.* (This article's discussion of blockchain does not provide an overview of nodes.)
16. *Id.*
17. *Id.*
18. Rebecca M. Bratspies, *Cryptocurrency and the Myth of the Trustless Transaction*, MICH. TELECOMM. TECH. L. REV. 1, 20 (2018).
19. NAKAMOTO, *supra* note 12, at 2–3.
20. *Id.* at 2.
21. *Id.*
22. *See generally id.*
23. *Id.* at 4.
24. Carol Goforth, *The Lawyer's Cryptionary: A Resource for Talking to Clients About Crypto-transactions*, 41 CAMPBELL L. REV. 47, 88 (2019).
25. *Id.* at 88–89.
26. *Id.* at 89.
27. *See generally id.*; NAKAMOTO, *supra* note 12, at 4.
28. Goforth, *supra* note 24, at 64.
29. "'Cryptocurrency' is a term that is not always used to mean precisely the same thing." *Id.* at 69.
30. *See generally id.* at 52.
31. *Id.*
32. *Id.* at 75.
33. Adam Sulkowski, *Blockchain, Business Supply Chains, Sustainability, and Law: The Future of Governance, Legal Frameworks, and Lawyers?*, 43 DEL. J. CORP. L. (forthcoming 2019).
34. *Id.*
35. *Id.*
36. *See generally* Goforth, *supra* note 24, at 84.
37. *Id.*
38. *Id.*
39. *Id.*
40. Alan Cohn, Travis West & Chelsea Parker, *Smart After All: Blockchain, Smart Contract, Parametric Insurance, and Smart Energy Grids*, 1 GEO. L. TECH. REV. 273, 277–78 (2017).
41. *Id.*
42. *Id.*

43. *See generally* Adam J. Kolber, *Not-So-Smart Blockchain Contracts and Artificial Responsibility*, STAN. TECH. L. REV. P198 (2018).
44. *Id.*
45. AUGUR, www.augur.net (last visited Apr. 17, 2019).
46. Goforth, *supra* note 24, at 69.
47. GOLEM, https://golem.network (last visited Apr. 4, 2019).
48. Goforth, *supra* note 24, at 97–99.
49. *See, e.g.*, COINBASE, www.coinbase.com (last visited Apr. 20, 2019).
50. Goforth, *supra* note 24, at 80–82.
51. *Id.*
52. *Id.* at 58.
53. *Id.*; Axel Hodler, *Proving Ownership of a Cryptocurrency*, MEDIUM (Aug. 8, 2017), https://medium.com/yopiter/proving-ownership-of-a-cryptocurrency-86a96f2c52b.
54. Cohn et al., *supra* note 40, at 277–79.
55. Goforth, *supra* note 24, at 112–14.
56. *Id.*
57. Doug Alexander, *Crypto Exchange Founder Dies, Leaving Behind $200M Problem*, ACCOUNTING TODAY (Feb. 5, 2019), www.accountingtoday.com/articles/crypto-exchange-founder-dies-leaving-behind-200m-problem.
58. *Id.*
59. *Id.*
60. Sulkowski, *supra* note 33.
61. *Id.*
62. *Id.*
63. *Id.*
64. Frank Etto, *Know Your Coins: Public vs. Private Cryptocurrencies*, NASDAQ (Sept. 22, 2017), www.nasdaq.com/article/know-your-coins-public-vs-private-cryptocurrencies-cm849588.
65. *Id.*
66. *Id.*
67. *Id.*
68. *See generally* Jason Bloomberg, *Using Bitcoin or Other Cryptocurrency to Commit Crimes? Law Enforcement Is onto You*, FORBES (Dec. 28, 2017), www.forbes.com/sites/jasonbloomberg/2017/12/28/using-bitcoin-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you/#6c84cf123bdc.
69. Etto, *supra* note 64.
70. Internal Revenue Service Notice 2014-21.
71. *Id.*
72. *Id.*
73. *Id.*
74. *Id.*
75. Goforth, *supra* note 24, at 104.
76. Bratspies, *supra* note 18, at 46.
77. *Id.*
78. *Id.*
79. *Id.*
80. *TurnKey Jet, Inc.* No-Action Letter from the U.S. Sec. & Exch. Comm'n, Div. of Corp. Fin. (Apr. 3, 2019), www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm.
81. *Id.*
82. di Liscia, *supra* note 1.
83. *Id.* at IV.

84. *Cryptocurrency Insurance Guide*, BITIRA (Oct. 9, 2018), www.bitira.com/cryptocurrency-insurance-guide.
85. *Id.*
86. Kimmelman v. Wayne Ins. Grp., 2018 Ohio Misc. LEXIS 1953 (2018).
87. di Liscia, *supra* note 1, at IV.
88. Bratspies, *supra* note 18, at 17.
89. *Id.*
90. *Id.*
91. *Id.*
92. di Liscia, *supra* note 1.
93. *Id.*
94. *Id.*
95. Michael Abramowicz, *Cryptoinsurance*, 50 WAKE FOREST L. REV. 671 (2015); Larry Schiffer, *Blockchain Technology and Reinsurance*, IRMI (Mar. 2017), www.irmi.com/articles/expert-commentary/blockchain-technology-and-reinsurance.
96. Cohn et al., *supra* note 40.
97. *Id.*