BLOCKCHAIN 101


By Jason Lewis, of Counsel, Partner, and Michael Loesch, Partner, Winston & Strawn, LLP

These days, it's hard to avoid the hype surrounding blockchain technology. One fintech executive has likened blockchain technology to "e-mail for money."[1] The World Economic Forum stated as early as 2015 that "[t]he blockchain protocol threatens to disintermediate almost every process in financial services."[2] Technology analyst International Data Corporation has predicted that over the period from 2016 through 2021, blockchain spending will grow at a five-year compound annual growth rate of 81.2%, with total spending in 2021 of $9.7 billion[3]. Yet, as the New York Times Magazine reported earlier this year, "the hype cycles are so accelerated that billions of dollarsare chasing a technology that almost no one outside the cryptocommunity understands, much less uses."[4]

Given the potential impact of these new technologies and the market's enthusiasm for them, this article attempts to help newcomers with the challenge of separating the facts about blockchain technology from the fiction. We first explain some blockchain basics: what blockchain technology is; how it works; and how it relates to concepts like smart contracts, tokens and Initial Coin Offerings. Next, we describe the potential advantages and disadvantages of using blockchains in business processes. Part 2 of this article, which will appear in a future issue, will focus on applications of this technology to commodities, shipping and logistics.

BLOCKCHAIN BASICS

Distributed Ledger Technology

Blockchains are a form of "distributed ledger technology," often abbreviated as "DLT." A distributed ledger is a secure database in a decentralized system that contains records of transactions among system participants. In its purest form, all participants have a copy of the ledger, and all records in the ledger are immutable, but no central authority (like a bank determining whether a check has bounced) ensures the accuracy of the database. Instead, the system uses cryptography – the art and science of secure communications – to maintain the security of the ledger.

To some, this use of cryptography portends the elimination of centralized intermediaries like financial institutions. DLT boffins often imagine a "trustless" world, where one does not need to rely on the integrity of other market participants or financial institutions in order to transact. Such a trustless world might enable a wider range of ordinary business transactions across borders. But such technologies also threaten to reshape the internet itself, returning it once again to its "egalitarian" roots.[5]

What are blockchains and how do they work?

Blockchains rely upon a specific set of cryptographic techniques to link transactions on the distributed ledger in a manner that provides a unique promise of security. Below, we provide a brief summary of the principal technical concepts necessary to understand the potential applications of blockchains.[6]

In a blockchain, each transaction on the ledger is "hashed" into a "block" that refers back to a prior block, thus forming a "chain" of sorts. "Hashing" means that a certain type of cryptographic algorithm is used to take "input" data about the transaction and generate a string of characters that has a fixed length.[7] The hash functions used in blockchains have a variety of properties that makes them ideal for such use. First, these hash functions are "deterministic," such that the same result occurs every time you put the same input through a hash function, and hashes can be calculated quickly.[8] Relatedly, the process generally provides each set of inputs with its own hash, which experts refer to as "collision-resistant." [9] Second, it is infeasible to determine the original input from the output hash, which is known as "pre-image resistance,"[10] or the "hiding" property of hashes.[11] Third, small changes in the input lead to significant changes in the output hash.[12] Fourth, such hash functions are "puzzle friendly."[13] Puzzle friendliness means that the best strategy to a "search puzzle" using the hash function is to try random values until happening upon the solution.[14] A search puzzle requires the solver to find an input to the hash function such that, when combined with a number chosen at random from a large distribution, the input results in a hash that falls within a specified range.[15] Solving this type of puzzle is the goal of cryptocurrency "mining," discussed in further detail below.

A blockchain connects blocks by employing "hash pointers." A hash pointer is a string of data that contains both the address of the previous block[16] (i.e., its location on the blockchain) and a hash of the data inside that previous block. Each block in the chain contains data pertaining to the transaction that it is recording as well as a hash pointer referring to the previous block.[17] In other words, the hash of any block depends on the data from the previous block in the chain. In the event that a system participant attempts to alter data along the chain – for example, to falsify a transaction on the ledger or "double-spend" a coin – the changed data will no longer match up with the hash that already has been recorded in the subsequent block. As discussed above, an output hash is sensitive to any changes made to the input hash. Therefore, any attempt to tamper with the ledger (i.e., by changing the contents of a prior block in the chain) should be readily apparent to participants in the blockchain.[18] This ability to detect foul play is fundamental to the security of blockchains, which are thus considered to be "immutable."

> Blockchains threaten to reshape the internet itself, returning it once again to its "egalitarian" roots.

Additional cryptographic techniques record blocks sequentially on a distributed ledger as transactions occur. Each "node" (i.e., party on the system) uses a "digital signature" to authenticate messages between it and the other party to a transaction.[19] After the parties agree to transact with their digital signatures, a new block is added to the blockchain when the remaining nodes on the system validate the hash data for the new block through a "consensus mechanism." Two common consensus mechanisms are Proof of Work ("PoW"), which Bitcoin uses, and Proof of Stake ("PoS"), a variant of which the Etherium community has proposed to adopt in the near future.

The PoW mechanism incentivizes nodes to solve a search puzzle created by the proposed addition of a new block. It does so by rewarding a node with a small amount of newly created Bitcoin (and a small transaction fee) each time: (i) that node is the first to determine a value used only once (i.e., a "nonce") that, when combined with the hashes of the previous transactions in the chain, generates a new hash within a certain numerical range, and (ii) the other nodes on the system accept the block formed with the newly determined data.[20] This process of earning Bitcoin in return for generating new blocks is called "mining." By recruiting a robust network of nodes to participate in the process of validating blocks, and by pitting all the nodes against each other in a race to solve these search puzzles, this mechanism guards against the risk that a bad actor can control enough votes on the system to manipulate the consensus mechanism or otherwise destroy confidence in the ledger (also known as "51% attacks").[21]

Unlike PoW, PoS mechanisms select one or more validators for a new block based on the amount of a deposit that the validator agrees to forfeit if it violates certain pre-set rules.[22] In other words, nodes willing to risk a greater "stake" have a greater chance of being selected to validate transactions and earn fees.[23] Once a block is validated using PoS, the validator (or validators, depending on the precise PoS scheme) earns a transaction fee.[24] Because all the nodes on the system do not compete to validate every block, PoS uses computing resources and electricity more efficiently,[25] while potentially producing faster results.[26] PoS is controversial in the cryptocommunity, however, precisely because it does not permit all nodes to compete for rewards, like Bitcoin's PoW mechanism, and may allow the largest players to dominate a platform by posting the greatest deposits.

Blockchain networks exist in two general forms: "permissionless" blockchains and "permissioned" blockchains. In permissionless blockchains like Bitcoin or Ethereum, anyone may join the network and participate in the process of block verification.[27] The existence of unlimited and unknown participants in such systems requires the careful design of consensus mechanisms to validate transactions, but advocates proclaim that such systems are less fragile.[28] In contrast, permissioned blockchains limit the actors that can contribute to the system, and typically require a centralized third party to serve as the gatekeeper.[29] The category of permissioned blockchains includes both "private" and "consortium" blockchain networks. Private blockchain networks are established and maintained by a single enterprise, while consortium networks are created by a group of companies collectively involved in managing the system.[30] Systems also may exist in the future that combine features of permissionless and permissioned blockchains.

Smart Contracts: Neither Smart, Nor Contracts?

"Smart contracts" are related to DLT, but are not one and the same technology. The term has two different meanings, however, and often is used imprecisely. First, the term may refer to a set of computer code (sometimes called "smart computer code") that automatically executes one or more tasks upon the satisfaction of one or more conditions.[31] Computer scientist and cryptography expert Nick Szabo famously described this type of smart contract by analogy with a vending machine: when a buyer fulfills the condition by inserting a sufficient amount of coinage, the vending machine executes the condition by dispensing the requested product and, where appropriate, change.[32] Developers often embed this type of smart contract within a distributed ledger, such that the distributed ledger automatically records the execution (or not) of the tasks in question.[33]

Second, the term smart contract also may refer to a legally enforceable contract that either contains pieces of smart computer code or is constructed entirely of such code (sometimes called a "smart legal contract").[34] It has been said that "every smart legal contract can be said to contain one or more pieces of smart contract code, but not every piece of smart contract code comprises a smart legal contract."[35] Smart legal contracts thus are similar to smart computer code, but use that code within a binding legal relationship; upon a contractual breach, the aggrieved party can resort to the legal system to enforce that relationship. Smart legal contracts may be in written form, and contain traditional contractual provisions outside of those that have been programmed in smart computer code. Different models already exist for incorporating computer code into legally binding contracts, and given the close association between smart contracts and blockchains, are expected to mature as blockchain technology proliferates.[36]

Critically, however, any such provisions relying on smart computer code must be susceptible to an objective determination by a computer as to whether the relevant condition or conditions have been satisfied. (Where an outside source provides the information necessary for such a determination, such source is often referred to as an "oracle.") Like the vending machine analogy above, a smart contract can be designed to record a financially settled option transaction on a distributed ledger, for example, if the daily settlement price of a certain futures contract on a specified exchange (in this context, the "oracle") exceeds a certain strike price. But without some objective criteria – like the proper amount of coins to be placed in the slot – a smart contract would not have the ability to determine when a party has used "commercially reasonable efforts" to perform a contractual covenant, whether a party has negotiated an open provision "in good faith," or whether a "material adverse effect" has occurred.[37] Traditional contracts also contain "non-operational" clauses that do not necessarily document the logic of the transaction itself, but rather describe the legal relationship between the parties, such as provisions that specify the governing law or the venues in which the parties must or may bring any disputes.[38] At present, therefore, it may not be accurate to call such contracts "smart," since computer code cannot implement these provisions. But developers are working feverishly to implement this technology in an increasingly complex range of products.

Cryptocurrencies and Tokens

The blockchain world has progressed quickly, and – adding to the confusion – in many cases without a fundamental agreement on the meaning of key terms. Two of those key terms are "cryptocurrency" and "token," both of which have recently featured prominently in the news.

A cryptocurrency is "a form of digital money that is designed to be secure and, in many cases, anonymous."[39] Cryptocurrencies use blockchain technology to record the movement of currency among all system participants in a distributed ledger, and typically use software protocols that are unique to that blockchain. Notable examples include Bitcoin (built on the Bitcoin blockchain), Ether (built with the Etherium blockchain), XRP (built on the Ripple blockchain), and Litecoin (a "fork," or variation of, the Bitcoin blockchain). Compounding the confusion, cryptocurrencies are sometimes referred to as "coins" or "altcoins."

The term "token," on the other hand, may sometimes refer to a cryptocurrency generally, but more precise definitions of the term typically refer to programmable digital assets that confer actual property rights outside the blockchain or access to a function within a particular platform.[40] Tokens are usually developed using another blockchain (i.e., what some refer to as the "native" blockchain, like Bitcoin or Etherium) to facilitate the settlement of more complex "upper-layer" transactions on the relevant platform, and employ smart contracts to implement those transactions.[41] The Etherium blockchain, for example, was specifically designed to facilitate the creation of tokens and the use of smart contracts, and includes features that allow developers to create standardized tokens without recreating key pieces of computer code.[42] A token thus resembles a "store specific loyalty point,"[43] like frequent flier miles or "Starbucks Rewards," that can be redeemed only from that particular vendor. By way of analogy, many have compared tokens with a ticket at a fairground – within the fairground only, the bearer can redeem the ticket for cotton candy, ride the Ferris wheel, or play a game. Consider the following examples from three disparate industries:

• Basic Attention Token (BAT)

The BAT was created in 2016, using the Etherium protocol, to improve the internet advertisement industry. To accomplish this, the creators of BAT developed their own internet browser, called Brave, which has the ability to assess the time and attention that users spend viewing advertisements. On Brave, advertisers pay publishers for advertisements using BAT, with the amounts increasing based on the amount of attention that users give to an advertisement, while users are compensated with BATs for viewing those advertisements. BATs are tradable between system participants. BAT tokens are not restricted to a particular use, but the developers have suggested that publishers could allow users to redeem BATs for premium content, such as premium articles or higher quality video or audio content, that users could donate BATs to charity, or that BATs could be used in online games. The "Initial Coin Offering" (or "ICO") of the BAT in May 2017 generated approximately $35 million, and all of the tokens for sale had been purchased within thirty seconds.[44]

• TenX

TenX is a cryptocurrency payment platform that seeks to enable people to use cryptocurrencies in their everyday lives. TenX issues debit cards to users or allows users to fund a mobile "wallet" with Bitcoin, Ether, Litecoin or (in time) others. When a user enters into a transaction with the debit card or mobile wallet, the TenX network rewards the user with 0.1% of the transaction value in the form of PAY tokens; on a monthly basis, 0.5% of the aggregate transaction value on the TenX network is distributed to holders of PAY tokens in the form of Ether. TenX also was developed using the Etherium protocol.[45] In the June 2017 ICO of its PAY tokens, TenX raised $34 million in seven minutes.[46]

• Beercoins

Beercoins may be "mined" by scanning QF, NFC or text tags (either inside a bottle cap, on a coaster, or on the check from a participating bar or restaurant); system users may transfer the tokens to other system users on the "Beerchain," donate them to charity or redeem them through participating vendors for beer, discounts or merchandise.[47] Beercoin also was developed using the Etherium blockchain.[48] The Beercoin Foundation held an ICO that concluded on June 30, 2018; a second ICO is planned for September 2018.[49]

Initial Coin Offerings

An ICO, another term that has appeared in the news of late, is a method of crowdfunding that acts like an initial public offering of stock ("IPO"). In an ICO, the creator of a blockchain-based platform offers a token to the public for sale, usually within a specified period of time. Like the examples above, the tokens typically are for use on the platform that is attempting to raise capital, and typically are tradable, which allows buyers to take advantage of rising prices or causes them to incur losses when prices move against them. An offeror of tokens usually details its proposed system in a "whitepaper" that it posts to its website for public review. These whitepapers set forth the business case in favor of the token, and explain how the relevant platform works, but can vary substantially in quality and transparency. Once the token sale has occurred, the proceeds of the ICO compensate the founders, much like an IPO, but also raise money for the development or expansion of the relevant platform. This atmosphere is ripe for predatory practices, since in many cases that platform has not yet been developed, and is simply a concept described at the time of the ICO in a whitepaper.

Indeed, a host of legal issues have arisen as regulators around the world have considered the possibility for exploitative or fraudulent behavior in connection with ICOs and cryptocurrencies. The U.S. Securities and Exchange Commission in particular has taken an active role in reviewing proposed ICOs, and has determined that ICOs may constitute offerings of securities subject to its jurisdiction.[50] Similarly, the U.S. Commodity Futures Trading Commission has determined that Bitcoin and other virtual currencies are commodities, that derivative contracts with respect to such commodities are subject to its jurisdiction, and that trading of Bitcoin in interstate commerce is subject to laws prohibiting fraud and manipulation.[51] We expect these regulators and others to remain active as blockchain technology continues to evolve.

Potential Benefits and Challenges

Blockchain advocates point to a wide range of potential benefits from using the technology. Chief among those benefits are the following:

- **Transactional efficiency.** While it may not be the case today, enthusiasts can foresee a time when blockchain technology offers superior processing speeds and lower transaction costs. Blockchains also could reduce transactional friction from centralized authorities or other intermediaries like financial institutions; for example, by automating transactions through smart contracts, or relieving the need for duplicative data entry or records among participants in a supply chain.

- **Transactional transparency and reliability.** As discussed above, the distributed ledger is generally open to all participants, and records are irreversible and immutable; therefore, all participants should theoretically have a high degree of trust in the integrity of the ledger. Such enhanced transparency and reliability reduces the need for a commercial relationship between a buyer and seller, and may enable a wide range of "trustless" business transactions worldwide that do not require the participation of central authorities. These features also provide enhanced protection against cybercrime and fraud. In some cases, blockchains may even be designed to help users authenticate the identities of their counterparties.

- **Audit trail.** Because the distributed ledger is generally open to all participants, counterparties should have ready access to a full record of their transactions, thus enabling faster and more efficient reconciliation of settlement discrepancies and other disputes. Blockchains could revolutionize accounting, financial auditing or regulatory reporting as well.

- **New Business Models.** These new technologies and the ongoing flood of investment will no doubt result in new business models. We have perhaps only begun to see the benefits of blockchains.

On the other hand, several factors – in many cases, the same factors that confer advantages on blockchain-based systems – may challenge the widespread application of blockchains:

- **Slowness.** Blockchain technology is currently not as fast as existing settlement methods like credit cards. Nonetheless, it may not be appropriate to compare credit card processing and block validations, since the processing of a credit card transaction does not result in the immediate payment of money, but the validation of a transaction on the blockchain represents the actual movement of cryptocurrency or tokens. Improvement in the speed of blockchain formation also is likely in the future.

- **Security Issues.** Like other information technology systems, blockchains can present attractive targets for hackers. In particular, blockchain-based platforms must be designed thoughtfully to prevent hackers from launching "51% attacks" or exploiting other vulnerabilities.

- **Resource scarcity.** Blockchains may result in the inefficient allocation of computing resources or electricity. The nature of a distributed ledger necessarily implies that every "node" on the applicable system will store the same information, which will increase in size as the ledger grows with new blocks. In fact, such redundancy is a security feature of distributed ledgers. But such redundancy could use an inordinate amount of data storage. Validation processes based on consensus models also require participation from multiple nodes in order to ensure the security of those processes – especially in PoW systems, as discussed above. PoW systems provide incentives to deploy ever greater computing power in a ceaseless arms race among nodes, and may divert resources or electricity from more socially beneficial uses.

These new technologies will no doubt result in new business models. We have perhaps only begun to see the benefits of blockchains.

- **Lack of standardization.** Given the bloom of new blockchain applications across a wide range of industries, it is still too early to determine whether a single dominant platform will prevail in any industry, or whether multiple competing platforms will emerge. Potential users must therefore carefully evaluate the risks of early adoption. In the event that a user throws its weight behind a single platform, it is likely not clear whether that platform's blockchain will ever be "interoperable" with others. For example, users are left to wonder what will happen if they wish to novate transactions in the future to a counterparty that has not yet adopted that particular platform. Users also need to ask what happens to pending transactions on the chosen platform if that platform fails. This lack of standardization among competing platforms may keep users on the sidelines, and has attracted attention at the highest levels of government.

- **Anonymity.** Most blockchains are "pseudonymous" rather than anonymous, meaning that participants can identify other participants only by their "public keys," which do not reveal their underlying identities. Such use of pseudonyms is consistent with a marketplace where collective trust in cryptography supplants personal relationships. But certain legal regimes include "know your customer" requirements to prevent money laundering and other criminal activity, and even a relative degree of anonymity may preclude compliance with these requirements. A permissioned blockchain might solve this problem, such that a central administrator can facilitate compliance with these obligations, but permissioned blockchains may confer only some of the benefits described above if they merely replace one set of intermediaries with another.

- **Lack of Confidentiality.** As discussed above, a distributed ledger subject to review by all "nodes" can provide a powerful substitute for trust between market participants. But some transactional environments may require confidential treatment of contract terms or even the existence of a transaction. Unlike the problem with relative anonymity, described above, pseudonyms may not provide adequate confidentiality in these situations. For example, if a participant is able to correlate a transaction on the blockchain with its counterparty's pseudonym, it may be able to discern the identity of that counterparty. Like the problem with relative anonymity, however, a permissioned blockchain may address this issue.

- **Regulatory oversight.** Blockchains, cryptocurrencies and ICOs are potentially subject to regulation by a wide range of governmental agencies internationally, and pose significant regulatory challenges with respect to securities and commodities laws, trade sanctions, and banking laws, among others. The manner in which regulators deal with these issues could impact the development of blockchain technology and its application in many different contexts.

- **Pre-existing solutions.** In some cases, blockchain technology simply may be unnecessary, as existing, proven technology could accomplish a similar result.

Therefore, despite the market's ebullience, blockchain technology is, by any assessment, in the early stages of delivering upon its promises. As the applications of blockchain technology continue to evolve, it will likely become increasingly clearer to developers, users, and investors as to when a blockchain-based solution is best. In the meantime, much like the early days of the internet, we recommend that readers view the dizzying array of new business opportunities with a healthy degree of skepticism. ▲

We hope that this brief introduction to blockchain technology has provided readers with the background to approach the topic with greater confidence. In Part 2, that will be featured in Issue I, 2019, we will review some potential applications of blockchain technology, with a focus on commodities, shipping and logistics

1. Robinson, Edward And Leising, Matthew, *Blythe Masters Tells Banks The Blockchain Changes Everything,* BLOOMBERG (Aug. 21, 2015), https://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything.
2. *Id.*
3. *New Spending Guide Sees Worldwide Blockchain Spending Growing To $9.7 Billion In 2021*, IDC (Jan. 24, 2018), https://www.idc.com/getdoc.jsp?containerId=prUS43526618.
4. Johnson, Steven, *Beyond The Bitcoin Bubble,* THE NEW YORK TIMES Magazine (Jan. 16, 2018).
5. Johnson, *supra* n. 5.
6. For a more detailed and complete description of the basic concepts, see Narayanan, Arvind *et al., Bitcoin and Cryptocurrency Technologies* (Princeton University Press: 2016) at 1-20.
7. *What Is Hashing? Under The Hood Of Blockchain*, BLOCKGEEKS (Last Visited July 6, 2018), https://blockgeeks.com/guides/what-is-hashing/.
8. *Id.*
9. *Id.*
10. *Id.*
11. Narayanan *et al.* at 5.
12. BLOCKGEEKS, *supra* n. 7.
13. *Id.*; Narayanan *et al.* at 8.
14. Narayanan *et al.* at 8-9.
15. *Id.*
16. *Id.* at 10.
17. *Id.* at 11.
18. BLOCKGEEKS, *supra* n. 7; Narayanan *et al.* at 12.
19. Narayanan *et al.* at 15-18.
20. *Id.* at 104-110.
21. See, *id.* at 40-50.
22. *Proof Of Work Vs. Proof Of Stake: Basic Mining Guide*, BLOCKGEEKS (Last Visited July 10, 2018), https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.
23. Castor, Amy, *A (Short) Guide To Blockchain Consensus Protocols*, COINDESK (Last Visited July 10, 2018), https://www.coindesk.com/short-guide-blockchain-consensus-protocols/.
24. *Id.*
25. BLOCKGEEKS *supra* n. 23.
26. Kimathi, Basil, *Game Changer: Proof Of Stake Is Coming Fast*, CRYPTOLINE NEWS (Feb. 7, 2018), https://cryptolinenews.com/2018/02/proof-of-stake-is-coming-fast/.
27. Annamalai, Deva, *Blockchain – What Is Permissioned Vs. Permissionless?*, COREDUMP (Jan. 10, 2017), https://bornonjuly4.me/2017/01/10/blockchain-what-is-permissioned-vs-permissionless
28. *Id.*
29. *Id.*
30. Buterin, Vitalik, *On Public And Private Blockchains*, ETHEREUM BLOG (Aug. 6, 2015), https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.
31. ISDA and Linklaters, *Whitepaper: Smart Contracts And Distributed Ledger – A Legal Perspective* (Aug. 2017), https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf at 5.
32. *See* Szabo, Nick, *The Idea Of Smart Contracts*, NICK SZABO'S ESSAYS, PAPERS, AND CONCISE TUTORIALS (1997), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.
33. ISDA and Linklaters, *supra* n. 32.
34. *Id.*
35. *Id.*
36. *Id.* at 13-18.
37. *See id.* at 12.
38. *Id.* at 11.
39. *What Is Cryptocurrency, How Does It Work, And Why Do We Use It?*, THE TELEGRAPH (Last Visited July 10, 2018), https://www.telegraph.co.uk/technology/0/cryptocurrency/.
40. Aziz, *Coins, Tokens & Altcoins: What's The Difference?*, MASTERTHECRYPTO (Last Visited July 10, 2018), https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/.
41. *Id.*; Taché, Adam, *State Of Cryptocurrencies: Summer 2018*, HACKERNOON (June 23, 2018), https://hackernoon.com/state-of-cryptocurrencies-summer-2018-932016549375.
42. *See How Ethereum Works*, COINDESK (Last Visited July 10, 2018), https://www.coindesk.com/information/how-ethereum-works/.
43. Chester, Jonathan, *A New Way To Raise Money: The Initial Coin Offering*, FORBES (June 12, 2017), https://www.forbes.com/sites/jonathanchester/2017/06/12/a-new-way-to-raise-money-the-initial-coin-offering/.
44. Keane, Jonathan, *$35 Million In 30 Seconds: Token Sale For Internet Browser Brave Sells Out*, COINDESK (May 31, 2017), https://www.coindesk.com/35-million-30-seconds-token-sale-internet-browser-brave-sells/.
45. *See generally*, Buchko, Steven, *What Is Tenx? Beginner's Guide*, COIN CENTRAL (Dec. 2, 2017), https://coincentral.com/tenx-beginner-guide/; What Is TenX?, WEUSECOINS (last visited July 10, 2018), https://www.weusecoins.com/what-is-tenx/.
46. Iesho, Ashour, *Tenx Ico Raises $34 Million In 7 Minutes*, BITCOINIST (June 24, 2017), http://bitcoinist.com/tenx-ico-raises-34-million-7-minutes/.
47. BEERCOIN, https://www.beerchain.technology/ (Last Visited July 10, 2018).
48. *Id.*
49. *Beercoin, The Beer-Based Cryptocurrency*, ICOBENCH (Last Visited July 10, 2018), https://icobench.com/ico/beercoin.
50. *See*, Clayton, Jay, *Statement On Cryptocurrencies And Initial Coin Offerings*, U.S. SECURITIES AND EXCHANGE COMMISSION (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.
51. *See, Bitcoin Basics*, U.S. COMMODITY FUTURES TRADING COMMISSION, https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/oceo_bitcoinbasics0218.pdf.