Volume 1, No. 3 | May–June 2018

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL

The Journal of Robotics, Artificial Intelligence & Law

Volume 1, No. 3 | May–June 2018

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2018 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquires and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@
meyerowitzcommunications.com, 718.224.2258.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please call:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com
or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Taking Stock of the Block: Blockchain, Corporate Stock Ledgers, and Delaware General Corporation Law—Part I

John C. Kelly and Maximilian J. Mescall*

Delaware recently amended the Delaware General Corporation Law to authorize Delaware corporations to replace their paper and electronic stock ledgers with a blockchain. Blockchain, also known as a distributed ledger, can promote efficient recordkeeping, but there are several legal and practical hurdles that corporations need to address before they can reap the full benefits of blockchain legalization. In this first part of a two-part article, the authors discuss blockchain and its applications. The second part of the article, which will appear in an upcoming issue of The Journal of Robotics, Artificial Intelligence & Law, *will explain Delaware's legislation, and blockchain's potential uses and hurdles.*

Delaware recently amended the Delaware General Corporation Law ("DGCL") to explicitly authorize Delaware corporations to replace their paper and electronic stock ledgers with a blockchain. The law received acclaim from experts in the technological, corporate, and legal fields, and supporters expect it will reduce corporate transactional times and costs while avoiding expensive litigation. Because Delaware is the home of 64 percent of Fortune 500 companies and 90 percent of initial public offerings, the new amendment will have national implications.[1] Blockchain, also known as a distributed ledger, can promote efficient recordkeeping, but there are several legal and practical hurdles that corporations need to address before they can reap the full benefits of blockchain legalization.

Blockchain is the foundation of Bitcoin and Ethereum, two major cryptocurrencies that have shaken the basic assumptions underlying the financial industry. Bitcoin is to blockchain what email is to the internet: a single application to an expansive and disruptive technology. Just as the internet has shaken assumptions in commercial, informational, and service-based industries, blockchain challenges the foundations of financial industries and corporations. With its other evolving applications, such as Ethereum's

Robotics, Artificial Intelligence & Law / May–June 2018, Vol. 1, No. 3, pp. 145–159.
© 2018 Full Court Press. All rights reserved.
ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

Smart Contract program, blockchain may be able to fuel major innovations in the financial and corporate sphere.[2] Bitcoin has a checkered history and is often associated with criminal enterprises, such as tax evasion and drug smuggling. But Delaware's law removes blockchain from this legal gray area, enabling companies to use distributed ledgers in corporate governance and maintenance.[3] Corporations must utilize this new technology to stay ahead of the competition. This two-part article discusses blockchain and its applications, Delaware's legislation, and blockchain's potential uses and hurdles.

Blockchain and Its Applications

Blockchain Generally

At its core, blockchain is a type of database. Both store information, which users retrieve and alter. Databases, however, are centralized servers; all users must access the database in order to retrieve its data.[4] With centralization comes vulnerability. While a centralized database can restrict users, it can also be overwhelmed by Denial of Service attacks, unilaterally altered by the entity controlling the database or a malicious third party, or shut down if it malfunctions. Additionally, the owner of the database must pay for maintenance and upgrades on the system. System owners pass these expenses onto users or advertisers, driving up costs. In return for viewing advertisements or paying fees, users look to the trusted party, the database owner, to verify the information or transactions that take place on the database.[5]

Unlike an actual database, a blockchain is a decentralized ledger network.[6] Rather than having users access a single centralized database, users access the copy of the blockchain on their computer, which refreshes as other users access and update the content of the network.[7] By joining the network, users authorize their computers to become network nodes that verify transactions and alterations to the blockchain.[8] The blockchain "algorithmically enforce[s] private agreements and community principles at a global scale by shifting the cost of trust and coordination to the network."[9] Because nodes must authenticate each transaction, an exchange on a blockchain is considered trustless.[10] The network, rather than trusted third party, confirms an exchange.[11] Thus, person-to-person interactions are viable on a blockchain.

Instead of relying on a trusted party to verify transactions, the blockchain ensures accuracy by using cryptography and the hash function.[12] A hash function "enjoy[s] the potential for high security absent dedicated, and resource-intensive, attempts to crack them"[13] and allows users to detect tampering by malicious parties.[14] A hash function is too complex to explain entirely here, but essentially takes the input data, which are the transactions, and condenses them into secure output data, which is later organized into a block of information.[15] This block is then verified by computers on the network, which then hash—or chain—the blocks together.[16] If a hacker attempts to reverse a transaction, then the hashes between the various blocks change, alerting users that the new block is different from that which the blockchain accepted.[17] Additionally, that hacker would need to change every block in the chain, compromising multiple hashes and requiring an immense amount of computing power, with the power requirement increasing as the blockchain lengthens.[18] As a result, blockchains, though not infallible, are nearly impossible to alter.

There are three types of distributed ledgers a network creator can adopt: public, private, and hybrid (also known as consortium).[19] Public, or permissionless, ledgers are available to all, and all users have "identical privileges to view, modify and affix their assent to a transaction."[20] Private, or permissioned, ledgers allow access to a limited number of nodes, thereby controlling who may alter the blockchain.[21] Hybrid ledgers attempt to merge the transparency of public blockchains with the control of private ledgers by allowing a governing body to select which transactions are public and which require permission to view.[22] Blockchains are therefore customizable and can fit the needs of the parties or corporation that codes it.

Blockchain and Bitcoin

For those who have difficulty conceptualizing a blockchain, Bitcoin provides a real-world example of its function. Bitcoin is a type of cryptocurrency whose value is driven by speculation and scarcity, rather than by support from a government. It was first proposed by a person or group of people calling themselves Satoshi Nakamoto.[23] Utilizing distributed ledger technology, Nakamoto envisioned a system that allowed transactions without a trusted third party, such as a bank, reviewing and approving the exchange.[24] Essentially, Nakamoto suggested that cryptocurrencies could replace banks and government controls in the same way the blockchain could replace centralized databases.[25] With blockchain, once a transaction is made, it is nearly impossible to reverse.[26] Thus, a party cannot renege on a transaction once it occurs, and every user can trace the history of all bitcoins from creation to current ownership by examining the transactional history in the publicly viewable distributed ledger.[27]

To trade Bitcoin, users download a bitcoin wallet—a platform that grants access to the distributed ledger. There are two ways to put a bitcoin in this wallet: (1) trading real-world currency for bitcoin or (2) mining bitcoin.[28] Bitcoin mining is what drives the system and ensures the accuracy of the distributed ledger. When a transaction occurs, that transaction is added to a block with one block created about every ten minutes.[29] When a block is created, it is sent to nodes on the ledger, which then have an opportunity to mine the block.[30] Mining involves solving the difficult mathematical formulas that are the basis of cryptography.[31] Upon receiving the new block, Bitcoin miners engage in proof of work—a race to solve the cryptographic formula through pure computational guesswork.[32] The first user to solve the mathematical formula attempts to place the mined block on the largest chain on the ledger.[33] Using consensus protocols, the miner's node shares the mathematical answer to the cryptographic formula.[34] Once a majority of nodes accept the miner's answer as correct, the mined block is added to the longest chain.[35] In return for completing the equation first, the system may reward the miner with a newly minted bitcoin.[36] The ledger subsequently updates and supplies the miner with a pair of cryptographic keys specific to the bitcoin.[37]

These keys prove ownership of the bitcoin and are essential to the transfer processes.[38] Each bitcoin has a public key, which is what appears on the blockchain and is universally available to those who access the chain.[39] The owner of the cryptocurrency also has a private key, which acts like a password and is necessary to trade the coin.[40] A party obtains a bitcoin by communicating with a public key on the distributed ledger, and the owner confirming the trade by sending the private key to the blockchain.[41] When an owner trades a bitcoin, the blockchain "utilizes mathematical techniques to match a public address with a private security access key for each participant in a transaction."[42] Once the system verifies the public and private keys, the transaction is broadcast to all ledgers on the network, which group it with other transactions into a block that miners subsequently verify and place on the ledger.[43]

Cryptocurrencies are not necessary for a blockchain.[44] Innovative uses arise when the traded item is not a digital currency, but instead a digital representation of a real-world item, such as a property deed or an intellectual property right.[45] With smart contracts, parties can easily transfer goods and money by automating the transactional process.

Blockchain and Smart Contracts

A smart contract is a computerized protocol that, when all prerequisites are met, executes the terms of the contract.[46] It is therefore self-enforcing and can self-execute without significant input from either party.[47] Self-executing contracts have been around for decades, but the recent merger of blockchain and smart contracts have breathed new life into the technology. Along with blockchain's immutable ledgers, "[s]mart contracts can provide automatic and predictable execution, again removing the ability for third parties to subvert agreed-upon processes."[48]

Like its legal namesake, a smart contract contains clauses, such as bonding or collateral clauses, in the code itself.[49] Each of these programs has a unique address on the blockchain toward which the parties direct their transaction.[50] For example, some musicians have replaced record labels with smart contracts.[51] Listeners on a public blockchain submit a request to a smart contract for a musician's song.[52] The smart contract recognizes the request, takes the required cryptocurrency from the listener's wallet, places that currency in the musician's wallet and sends the listener an MP3 file with the requested song.[53] This transaction is recorded on the blockchain and is publicly viewable.[54] The artist, therefore, can maintain licensing ownership of the music, without a music label intermediary, and the listener can obtain the music at a fraction of the cost.[55]

In fact, smart contracts allow entire organizations to exist solely on the blockchain. With Ethereum, a blockchain platform that includes smart contracts, groups can organize a decentralized autonomous organization ("DAO").[56] Users establish a DAO to finish a certain project and then request funds from the community, similar to how a corporation raises money by making a public offering.[57] To set up a DAO, users write a smart contract that governs the fundraising.[58] One person is designated as the owner of the DAO and acts as a CEO or president.[59] Participating investors send ether, Ethereum's cryptocurrency, to the smart contract, which then executes its terms and sends an ownership token to the investor.[60] In some cases, smart contracts act similarly to a Kickstarter and return the ether to the investors if the DAO fails to reach its fundraising goals within a specified time.[61] In other cases, the code provides digital keys that grant voting rights in a DAO, allowing users to vote to support or ratify certain DAO actions.[62] If enough members vote in favor of pursuing the considered action, a smart contract executes, and the task is distributed to DAO employees or the action is automatically taken.[63] Alternatively, the owner can alter the founding smart contract and appoint other users to have control over certain actions similar to how officers in a corporation are responsible for certain tasks.[64]

Smart contracts, therefore, can significantly decrease the time and effort involved in decision making or agreement execution. If programmed correctly, they lead to "increased speed and accuracy of business transactions, more efficient business operations, and better, quicker, and cheaper enforcement of contracts."[65] With smart contracts, ownership of digital rights are clear and the program cannot distribute, seize, transfer, or divest those rights without the proper input. Simplification and efficiency are possible with the automatic execution of smart contracts. Additionally, since the smart contract is part of the code, it is not subject to political or jurisdictional divisions. As one scholar described it, "[w]ith smart contracts, it is the code that is the law."[66]

If the code is law, however, then flaws in the code are also law. Smart contracts are not infallible. The average software has between 15 and 50 errors per 1,000 lines of code.[67] Because smart contracts are a relatively new form of software, the likelihood of error is nearly double that average.[68] This article discusses some of these security issues, but first examines how real-world companies—specifically, financial institutions—have adopted this technology.

Blockchain and Fintech

Financial technology, otherwise known as fintech, encompasses several technologies, including cryptocurrencies, blockchain, mobile banking applications, securities, and high-frequency trading. While most of these advancements simply increase speed or access for financial institutions or consumers, blockchain provides the opportunity to make significant changes to the financial landscape.[69]

Because blockchain platforms are used primarily in cryptocurrencies and other financial investment platforms, centralized financial services are vulnerable for disruption. For the most part, the financial transfer systems have not changed significantly in 150 years. Even though money transfers move rapidly in the internet era, consumers still require a financial intermediary to transfer money on a person's behalf.[70] Depending on the complexity and the institution, the transfers can take hours, or days, to complete.[71] With the blockchain, individuals can complete verifiable money transfers in minutes, not days.

The ATM network provides an example of blockchain's disruptive potential.[72] Each ATM is owned and operated by a single bank, but also accepts cards from other institutions. To handle withdrawals from other banks, a centralized intermediary, such as Visa, processes the transaction and charges a transactional fee. With blockchain, the centralized intermediary is unnecessary. Bank ATMs can interact directly on the decentralized ledger to handle such requests. That is the type of disruption that Bitcoin was intended to create. "The question is not whether network business models supported by blockchain technology will disrupt [banking] organizations, but when."[73]

At this early adoption stage, rather than upending the financial system, financial institutions are adopting blockchain to make their systems more efficient.[74] Banking consortiums led by blockchain software developers, such as The Enterprise Ethereum Alliance, Ripple, R3, and Hyperledger, have organized to adopt blockchain for modern financial use.[75] While Bitcoin and Ethereum are versions of public ledgers, these financial blockchain initiatives have developed private blockchain ledgers.[76]

Using a private ledger, as opposed to a public or hybrid ledger, has several advantages in the financial industry. Some transactions, such as trade finance, remittances, syndicated lending, and treasury operations, require management by experts that only a private ledger allows.[77] With private ledgers, there is no need for Bitcoin's proof of work—the need to verify transactions via mining process—because all parties provided access are already incentivized to maintain accurate financial records. Additionally, banks can hide some transactions on the blockchain and allow their viewing by only approved individuals, thus protecting sensitive client data from public scrutiny.[78] Finally, while public blockchains are immutable, private ledgers may be altered at a later time to correct mistakes, assuming protocols are programmed into the system.[79]

Blockchain and Security

Public blockchains are perceived as immutable, but this perception overlooks several potential security risks. There are two types of security breaches—hacking critical nodes and 51 percent attacks—but there is also a corrective measure, known as a hard fork.

Electronic Infrastructure: The Electronic Components Surrounding Blockchains Are Still Vulnerable

Coindash, a blockchain trading platform, executed an initial coin offering ("ICO"), a type of initial public offering specific to cryptocurrencies, which allowed participants to send cryptocurrency to Coindash in return for its own digital tokens.[80] When the company placed the link to its electronic wallet on its website, a hacker altered the link, sending approximately $7 million in cryptocurrency to his personal wallet.[81] Coindash removed the fraudulent link and promised to provide investors with the tokens they purchased regardless of whether Coindash received the money; the hacker has yet to be caught.[82]

While established public blockchains such as Bitcoin and Ethereum are nearly impossible to alter, the digital infrastructure surrounding a blockchain is not equally secure. Individual nodes are hackable. Computers holding the private cryptographic keys for a bitcoin, for example, can be breached and the keys stolen, effectively pocketing the bitcoin itself.[83] Groups can hijack a system's proof of work power and create a separate longer blockchain to trick the blockchain into adopting the rouge chain.[84] Although a blockchain's whole is greater than the sum of its parts, software holes in the individual nodes that maintain the network can be exploited by third parties.

A 51 Percent Attack: Altering the Blockchain One Majority at a Time

Another vulnerability occurs when a person or group controls 51 percent of all the blockchain's processing power. Because 51 percent of all nodes must confirm that a block is valid before it can be added to a blockchain, control of over half of the network's computing power allows for manipulation of the data.[85] As a result, hackers could "revise recently settled transactions on the blockchain and prevent current and future transactions from being completed" effectively holding the blockchain hostage.[86] A 51 percent attack can occur when hackers control nodes maliciously. This can occur in one of two ways: either hackers collude to overtake a smaller cryptocurrency or hackers rent enough processing power to control a majority of the network's power. Because a blockchain's consensus protocol consumes large amounts of electricity, users tend to congregate in countries with low-cost electricity, increasing the possibility of a 51 percent attack through collusion.[87]

A 51 percent attack could occur on any network, but the smaller the network, the easier it is to control a majority of nodes. A smaller cryptocurrency known as Krypton was the first to suffer from such an attack.[88] Using superior hashing power, the hackers sold their Krypton and then rolled back the transactions, thus manipulating the ledger to show that the hackers received money for the exchange and still retained the cryptocurrency they just traded.[89] The hackers later held the Krypton network ransom and undermined user trust in the network.[90]

Because it was a smaller network, hackers required less computing power to seize Krypton's network than is required for larger cryptocurrencies, such as Bitcoin. However, a 51 percent attack is theoretically possible on any blockchain network.[91] When the Bitcoin community considered splitting into two separate currencies, Bitcoin and Bitcoin Unlimited, some who supported Bitcoin Unlimited suggested conducting a 51 percent attack on Bitcoin to undermine the currency and establish Bitcoin Unlimited's dominance.[92] The split never occurred, but enough centralized control of hashing power can undermine even large systems. The only way to correct such an attack is by convincing enough users to agree to a hard fork.[93]

The Hard Fork: A Corrective Action on a Public Ledger

A hard fork occurs when a node changes its underlying protocol but accepts the existing blockchain.[94] Subsequent transactions with this node diverge, or fork, from the nodes with the original protocol, thus creating two separate blockchains with the same original blocks.[95] Since a node can choose where to begin its divergence, a hard fork is one of the few effective ways to reverse fraudulent transactions.[96] Unfortunately, hard forks also occur when there is insufficient consensus from key nodes; when various computers disagree about whether to accept a transaction as legitimate, there is an inadvertent hard fork.[97]

Two major blockchain networks, Ethereum and Bitcoin, have conducted hard forks. The first, Ethereum, particularly showcases the security concerns surrounding blockchain and smart contracts. The first Ethereum DAO built its entire structure on the blockchain using smart contracts.[98] It raised money through a smart contract system, but software bugs in the smart contract allowed a hacker to drain $50 million, a third of the amount raised, into his personal account.[99] To remove the hack from the blockchain, a majority of users reverted to a prior blockchain, effectively erasing the transaction.[100] However, those that protested the reversal maintained the blockchain with the recorded theft, thus creating a hard fork.[101] Smart contracts, while efficient, are code that can be exploited if not properly built.

The second shows how difficult it is to maintain a public ledger. As Bitcoin aged, some users clamored for changes to the network's protocol to expand block size and mining speed.[102] When consensus failed, some miners created an offshoot cryptocurrency called Bitcoin Cash by changing a single node's protocol.[103] The subsequent hard fork split the database, confusing users and leaving Bitcoin brokers and exchanges scrambling for ways to handle transactions with both the original and new bitcoin.[104] With a public ledger, unanimous consensus is a must; otherwise, hard forks can effectively undermine the system.

* * *

The second part of this article, which will appear in an upcoming issue of *The Journal of Robotics, Artificial Intelligence & Law,* will explain Delaware's legislation, and blockchain's potential uses and hurdles.

Notes

* John C. Kelly (jkelly@mccarter.com) is a partner in the Business Litigation Practice Group at McCarter & English, LLP, representing companies, institutions, municipalities, and individuals with respect to all securities matters. Maximilian J. Mescall is a J.D. candidate, 2018, at Seton Hall University School of Law.

[1] Christopher Wink, *64% of Fortune 500 Firms are Delaware Incorporations: Here's Why,* Technically Delaware (Sept. 23, 2014), https://technical.ly/delaware/2014/09/23/why-delaware-incorporation/.

[2] Ryan Surujnath, *Off the Chain! A Guide to Blockchain Derivative Markets and the Implications on Systematic Risk,* 22 Fordham J. Corp. & Fin. L. 257, 279-84 (2017) (discussing how blockchain can impact derivative markets).

[3] Brian Patrick Eha, *Who Owns What, Really? In Securities, Delaware May Soon Clear Things Up,* American Banker (July 5, 2017), https://www.americanbanker.com/news/who-owns-what-really-in-securities-delaware-may-soon-clear-things-up.

[4] Surujnath, *supra* note 2 at 261.

[5] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2, https://bitcoin.org/bitcoin.pdf.

[6] Aaron Wright and Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* (Mar. 20, 2015) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 (describing blockchain as a decentralized database).

[7] Siraj Raval, *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology,* 45 (O'Reilly Media, Inc. 2016).

[8] *A Gentle Introduction to Blockchain Technology,* Bits on Blocks (Sept. 9, 2015), https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/.

[9] Patrick Murck, *Who Controls the Blockchain?,* Harvard Business Review (April 16, 2017), https://hbr.org/2017/04/who-controls-the-blockchain.

[10] Konstantinoes Christidis and Michael Devetsikiotis, *Blockchains and Smart Contracts for the Internet of Things,* 4 IEEE Access 2292, 2292 (2016), http://ieeexplore.ieee.org/document/7467408/?reload=true.

[11] Nakamoto, *supra* note 5 at 2.

[12] *See generally,* John Edward Silva, *An Overview of Cryptographic Hash Functions and Their Uses* (2003).

[13] Scott J. Shackelford & Steve Myers, *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace,* 19 Yale J. L. & Tech. 334, 384 (2017).

[14] Elizabeth Sara Ross, *Nobody Puts Blockchain in a Corner: The Disruptive Role of Blockchain Technology in the Financial Services Industry and Current Regulatory Issues,* 25 Cath. U. J. L. & Tech. 353, 363 (2017).

[15] New Zealand Blockchain Association, *If You Understand Hash Functions, You'll Understand Blockchains,* Decentralize Today (Nov. 29, 2016), https://decentralize.today/if-you-understand-hash-functions-youll-understand-blockchains-9088307b745d.

[16] Larissa Lee, *New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market,* 12 Hastings Bus. L.J. 81, 94-97 (2016); *The Great*

Chain of Being Sure About Things, The Economist (Oct. 31, 2015), https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

[17] *Id.*

[18] *Id.*

[19] Collin Thompson, *The Difference Between a Private, Public & Consortium Blockchain,* Blockchain Daily News, http://www.blockchaindailynews.com/The-difference-between-a-Private-Public-Consortium-Blockchain_a24681.html (accessed on Aug. 7, 2017).

[20] Rajashekara V. Maiya, *Public, Private or Hybrid Blockchain: What Does It Mean?,* DataQuest (May 10, 2017), http://www.dqindia.com/public-private-or-hybrid-blockchain-what-does-it-mean/.

[21] Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operation Risk,* 18 N.Y.U. J. Legis. & Pub. Pol'y 837, 840 n.15 (2015).

[22] Maiya, *supra* note 20.

[23] Nakamoto, *supra* note 5 at 1.

[24] *Id.*

[25] *Id.* at 2.

[26] Gideon Greenspan, *The Blockchain Immutability Myth,* LinkedIn (May 4, 2017), https://www.linkedin.com/pulse/blockchain-immutability-muth-gideon-greenspan.

[27] *See generally,* Catherine Martin Christopher, *The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain,* 17 Nev. L.J. 139 (2016) (discussing Bitcoin security).

[28] Sean McLeod, *Bitcoin: The Utopia or Nightmare of Regulation,* 9 Elon L. Rev. 553, 556 (2017).

[29] Garry Gabison, *Policy Considerations for the Blockchain Technology Public and Private Applications,* 19 SMU Sci. & Tech. L. Rev. 327, 340-41 (2016).

[30] *Id.*

[31] Elizabeth E. Lambert, *The Internal Revenue Service and Bitcoin: A Taxing Relationship,* 35 Va. Tax Rev. 88, 94-95 (2015).

[32] Lee, *supra* note 16 at 101-02.

[33] Lambert, *supra* note 31 at 95.

[34] Ronald Chan, *Consensus Mechanisms used in Blockchain,* LinkedIn (May 2, 2016), https://www.linkedin.com/pulse/consensus-mechanisms-used-blockchain-ronald-chan.

[35] *Id.*

[36] Lambert, *supra* note 31 at 94.

[37] Benjamin W. Akins, Jennifer L. Chapman, and Jason M. Gordon, *A Whole New World: Income Tax Considerations of the Bitcoin Economy,* 12 Pitt. Tax Rev. 25, 30 (2014).

[38] Mark Edwin Burge, *Apple Pay, Bitcoin, and Consumers: The ABCs of Future Public Payments Law,* 67 Hastings L.J. 1493, 1546 (2016).

[39] Marc Pilkington, Blockchain Technology Principles and Applications, at 4-5 (Sept. 18, 2015) (unpublished manuscript), https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2662660.

[40] Nicholas J. Ajello, *Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination,* 80 Brooklyn L. Rev. 435, 436-437 (2015).

[41] Jerry Brito, Houman Shadab, and Andrea Castillo, *Bitcoin Financial Regulation: Securities Derivatives, Prediction Markets, and Gambling,* 16 Colum. Sci. & Tech. L. Rev. 144, 149-150 (2014).

[42] Reggie O'Shields, *Smart Contracts: Legal Agreements for the Blockchain,* 21 N.C. Banking Inst. 177, 180 (2017).

[43] Jerry Brito, Houman Shadab, and Andrea Castillo, *Bitcoin Financial Regulation: Securities Derivatives, Prediction Markets, and Gambling,* 16 Colum. Sci. & Tech. L. Rev. 144, 149-150 (2014).

[44] Christidis, *supra* note 10 at 2293.

[45] Andrea Tinianow and Caitlin Long. *Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance,* Harvard Law Forum (March 16, 2017), https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance/ (discussing government uses of blockchain).

[46] Fiammetta S. Piazza, *Bitcoin and the Blockchain as Possible Corporate Governance Tools; Strengths and Weaknesses,* 5 Penn St. J. L. & Int'l Aff. 262, 296-97 (2017).

[47] Surujnath, *supra* note 2 at 271.

[48] Vinay Gupta & Rob Knight, *How Blockchain Could Help Emerging Markets Leap Ahead,* Harvard Business Review (May 17, 2017), https://hbr.org/2017/05/how-blockchain-could-help-emerging-markets-leap-ahead.

[49] Christidis, *supra* note 10 at 2296.

[50] *Id.*

[51] Ben Dickson, *Blockchain Could Completely Transform the Music Industry,* VentureBeat (Jan. 7, 2017), https://venturebeat.com/2017/01/07/blockchain-could-completely-transform-the-music-industry/.

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] Schumpeter, *Not-So-Clever Contracts,* The Economist (July 28, 2016), http://www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted.

[57] Seth Bannon, *The Tao of "The DAO" or: How the Autonomous Corporation is Already Here,* TechCrunch, https://techcrunch.com/2016/05/16/the-tao-of-the-dao-or-how-the-autonomous-corporation-is-already-here/.

[58] How to Build a Democracy on the Blockchain, Ethereum, https://www.ethereum.org/dao (accessed on Aug. 7, 2017).

[59] *Id.*

[60] Gertrude Chavez-Dreyfuss, *Virtual Company May Raise $200 Million, Largest in Crowdfunding,* Reuters (May 17, 2016), http://www.reuters.com/article/us-blockchain-crowdfunding-idUSKCN0Y82LI.

[61] Ameer Rosic, *Ethereum vs Bitcoin: What's the Main Difference?,* HuffingtonPost (Dec. 20, 2016), http://www.huffingtonpost.com/ameer-rosic-/ethereum-vs-bitcoin-whats_b_13735404.html.

[62] Schumpeter, *supra* note 56.

[63] Ethereum, *supra* note 58.

[64] *Id.*

[65] O'Shields, *supra* note 42 at 183.

[66] Ross, *supra* note 14 at 367.

[67] Schumpeter, *supra* note 56.

[68] *Id.*

[69] *But see* Danielle Andrus, *Why the Bitcoin Blockchain Won't Transform Financial Services,* ThinkAdvisor (March 9, 2017), http://www.thinkadvisor.com/2017/03/09/why-the-bitcoin-blockchain-wont-transform-financia.

[70] Rep. of World Econ. Forum, *The Future of Financial Services,* 43 (June 2015), http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf.

[71] *Id.*

[72] Vinay Gupta, *The Promise of Blockchain Is a World Without Middlemen,* Harvard Business Review (Mar. 6, 2017), https://hbr.org/2017/03/the-promise-of-blockchain-is-a-world-without-middlemen.

[73] Barry Libert, Megan Beck, and Jerry Wind, How Blockchain Technology Will Disrupt Financial Services Firms, Knowledge@Wharton (May 24, 2016), http://knowledge.wharton.upenn.edu/article/blockchain-technology-will-disrupt-financial-services-firms/.

[74] *Id.*

[75] Penny Crosman, *Banks Pour $107M into Blockchain Consortium R3,* American Banker (May 23, 2017), https://www.americanbanker.com/news/banks-pour-107m-into-blockchain-consortium-r3.

[76] Anna Irrera, *The Public vs Private Debate on Blockchain,* Financial Times (Sept. 28, 2015), https://www.fnlondon.com/articles/blockchain-fintech-the-public-vs-private-debate-20151001.

[77] Maiya, *supra* note 20.

[78] Irrera, *supra* note 76.

[79] Finextra Research, *Banking on Blockchain: Charting the Progress of Distributed Ledger Technology in Financial Services* (Jan. 2016), https://www.ingwb.com/media/1609652/banking-on-blockchain.pdf.

[80] Jen Wieczner, *Hackers Just Stole $7 Million in a Brazen Ethereum Cryptocurrency Heist,* Fortune (July 18, 2017), http://fortune.com/2017/07/18/ethereum-coindash-ico-hack/.

[81] Alexandria Arnold, *CoinDash CEO Says Ignore the Conspiracies After Coin-Sale Hack,* Bloomberg (July 20, 2017), https://www.bloomberg.com/news/articles/2017-07-20/coindash-ceo-says-ignore-the-conspiracies-after-coin-sale-hack.

[82] *Id.*

[83] Raja Raman and Mahesh Mangnaik, *Blockchain Can Transform The World, But Is It Fool-Proof?,* HuffingtonPost (Jan. 23, 2017), http://www.huffingtonpost.in/raja-raman/blockchain-can-transform-the-world-but-is-it-fool-proof_a_21660586/.

[84] *Id.*

[85] *Id.*

[86] Walch, *supra* note 21 at 861.

[87] Allison Berke, *How Safe Are Blockchains? It Depends,* Harvard Business Review (Mar. 7, 2017), https://hbr.org/2017/03/how-safe-are-blockchains-it-depends.

[88] Rocky, *Krypton Recovers From a New Type of 51% Network Attack,* CRYPTOHUSTLE (Aug. 26, 2016), https://cryptohustle.com/krypton-recovers-from-a-new-type-of-51-network-attack.

[89] *Id.*

[90] Rocky, *51% Attack Crew Extorts and Hijacks Blockchains for Ransom,* CRYPTOHUSTLE (Sept. 3, 2016), https://cryptohustle.com/51-attack-crew-extorts-and-hijacks-blockchains-for-ransom.

[91] Aaron van Wirdum, *Bitcoin Unlimited Miners May Be Preparing a 51% Attack on Bitcoin,* BITCOIN MAGAZINE (Mar. 29, 2017), https://bitcoinmagazine.com/articles/bitcoin-unlimited-miners-may-be-preparing-51-attack-bitcoin/.

[92] *Id.*

[93] Michael Abramowicz, *Cryptocurrency-Based Law,* 58 ARIZ. L. REV. 359, 382-383(2016).

[94] *Id.* at 381-82

[95] Walch, *supra* note 21 at 866.

[96] Surujnath, *supra* note 2 at 298.

[97] Frances Coppola, *Ethereum's Latest Hard Fork Shows It Has A Very Long Way To Go,* FORBES (Nov. 26, 2016), https://www.forbes.com/sites/francescoppola/2016/11/26/ethereums-latest-hard-fork-shows-it-has-a-very-long-way-to-go/#90e40af443a6.

[98] ETHEREUM, *supra* note 58.

[99] Jonathan Chester, *Will the $50m Heist of the DAO Take Down Bitcoin's Rival Blockchain?,* FORBES (Jun. 21, 2016), https://www.forbes.com/sites/jonathanchester/2016/06/21/can-the-50m-heist-of-the-dao-take-down-bitcoins-rival-blockchain/#4245d6bb7e37.

[100] Alex Sunnarborg, *In the Aftermath of the Ethereum Hard Fork Prompted by the DAO Hack, the Outvoted 15% are Rising Up with an Alternate Blockchain Worth $200 Million,* LINKEDIN (August 1, 2016), https://www.linkedin.com/pulse/aftermath-ethereum-hard-fork-prompted-dao-hack-15-up-worth-alex.

[101] Pete Rizzo, *Ethereum's Two Ethereums Explained,* COINDESK (July 28, 2016), https://www.coindesk.com/ethereum-classic-explained-blockchain/.

[102] James Titcomb, *Bitcoin Cash: Price of New Currency Rises After Bitcoin's 'Hard Fork',* THE TELEGRAPH (Aug. 2, 2017), http://www.telegraph.co.uk/technology/2017/08/01/bitcoin-cash-everything-need-know-bitcoins-hard-fork/.

[103] *Id.*

[104] *Id.*