Block-by-Block:
Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace

Scott J. Shackelford JD, PhD* & Steve Myers, PhD**

19 YALE J. L. & TECH. 334 (2017) (forthcoming)

There has been increasing interest in the transformative power of not only crypto-currencies like Bitcoin, but also the technology underlying them—namely blockchain. To the uninitiated, a blockchain is a sophisticated, distributed online ledger that has the potential, according to Goldman Sachs, to "change 'everything.'" From making businesses more efficient to recording property deeds to engendering the growth of 'smart' contracts, blockchain technology is now being investigated by a huge range of organizations and is attracting billions in venture funding. Even the U.S. Defense Advanced Research Projects Agency (DARPA) is investigating blockchain technology to "create an unhackable messaging system." However, the legal literature has largely ignored the rise of blockchain technology outside of its finance, securities, and copyright implications. This Article seeks to address this omission by analyzing the potential impact of blockchain technology on advancing the cybersecurity of firms across an array of sectors and industries with a particular focus on certificate authorities and the critical infrastructure context. Moreover, we examine the rise of blockchains through the lens of the literature on polycentric governance to ascertain what lessons this research holds to build trust in distributed systems and ultimately promote cyber peace.

Table of Contents

"Why should you care? Maybe you're a music lover who wants artists to make a living off their art. Perhaps you're an immigrant who's sick of paying big fees on remittances. Maybe you're an aid worker who needs to identify landowners so you can rebuild their homes after an earthquake. Or a citizen fed up with the lack of transparency and accountability of politicians. Or a social media user who thinks the data you generate might be worth something—to you. Even as we write, innovators are building blockchain-based applications that serve these ends. And they are just the beginning."

-Don Tapscott & Alex Tapscott, authors of *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World*[1]

INTRODUCTION

There has been increasing interest in the transformative power of not only crypto-currencies like Bitcoin,[2] but also the technology underlying them—namely blockchain.[3] Though Bitcoin gets most of the press, blockchains arguably enjoy the far greater potential to transform business and potentially revolutionize cybersecurity; simply put, according to Goldman Sachs, it could "change 'everything.'"[4] To the uninitiated, a blockchain is a sophisticated, distributed online ledger. From making businesses more efficient to recording property deeds to engendering the growth of "smart" contracts and even securing medical devices,[5] blockchain technology is now being investigated by a huge range of organizations and is attracting billions in venture funding.[6]

---

1 Don Tapscott & Alex Tapscott, *How the Technology Behind Bitcoin is Changing Money, Business and the World*, TIME (May 6, 2016), http://time.com/4320254/blockchain-tech-behind-Bitcoin/ [https://perma.cc/6BX9-EFEA].

2 *See, e.g.*, Luke Graham, *India's Rupee Restrictions are Boosting Demand for Bitcoin*, CNBC (Nov. 15, 2016, 8:44 AM), http://www.cnbc.com/2016/11/15/india-rupee-restriction-boost-Bitcoin-digital-currency.html [https://perma.cc/K4VN-S6NR].

3 *See* Naomi Lachance, *Not Just Bitcoin: Why The Blockchain Is a Seductive Technology To Many Industries*, NPR (May 4, 2016, 7:01 AM), http://www.npr.org/sections/alltechconsidered/2016/05/04/476597296/not-just-Bitcoin-why-blockchain-is-a-seductive-technology-to-many-industries [https://perma.cc/3CCX-L3GW].

4 *Id.*

5 *See* Asha McLean, *ASX Argues Medical Records Are Ripe for Blockchain*, ZDNET (Nov. 16, 2016, 22:00 PST), http://www.zdnet.com/article/asx-argues-medical-records-are-ripe-for-blockchain/ [https://perma.cc/BH7S-ZPNH].

6 *See* Kyle Torpey, *Prediction: $10 Billion Will Be Invested in Blockchain Projects in 2016*, COIN J. (Jan. 22, 2016), http://coinjournal.net/prediction-10-billion-will-be-invested-in-blockchain-startups-in-2016/

Even the U.S. Defense Advanced Research Projects Agency (DARPA) is investigating blockchain technology to "create an unhackable messaging system,"[7] as is IBM and Disney.[8] However, the legal literature has largely ignored the rise of blockchain technology outside of its finance, securities, and copyright implications.[9] This Article seeks to address this omission by analyzing the potential impact of blockchain technology on advancing the cybersecurity of firms across an array of sectors and industries with a particular focus on certificate authorities and the critical infrastructure context. Moreover, we examine the rise of blockchains through the lens of the literature on polycentric governance,[10] which reflects a blockchain's organization due to its focus on building trust in distributed systems as a tool to promote "cyber peace."[11]

In 1981, during what could be considered the predawn of the Information Age, researchers were already trying to solve varied privacy, security, and cryptographic concerns in the still nascent network.[12] Myriad techniques were tried, but regardless of the proposed solution, due to the involvement by third parties (such as credit card processors), insecurity persisted.[13] Some proponents even became jaded; one researcher, Nick Szabo, theorized a "God Protocol" in 1998 that

---

[https://perma.cc/TVN4-J6WY].

7 *See* Lachance, *supra* note 3.

8 Don Tapscott & Alex Tapscott, *Here's Why Blockchains Will Change the World*, FORTUNE (May 8, 2016), http://fortune.com/2016/05/08/why-blockchains-will-change-the-world [https://perma.cc/B9RV-MRMH].

9 Most articles to date have investigated the implications of blockchain technology in the financial market or copyright contexts. *See, e.g.*, Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 838 (2015) (discussing the operational risks undermining the utility of blockchains in certain financial contexts); Jeffrey E. Alberts & Bertrand Fry, *Is Bitcoin a Security?*, 21 B.U. J. SCI. & TECH. L. 1, 1, (2015) (investigating whether Bitcoin is a security); Nick Vogel, *The Great Decentralization: How Web 3.0 Will Weaken Copyrights*, 15 J. MARSHALL REV. INTELL. PROP. L. 136, 136 (2015) (analyzing the copyright implications of Bitcoin). Even those articles that have taken a wider view have only treated cybersecurity as an afterthought. *See* Trevor I. Kiviat, Note, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569, 601 (2016).

10 *See* Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39 POL'Y STUD. J. 163, 171 (2011).

11 Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 77, 82 (Hamadoun I. Touré & The Permanent Monitoring Panel on Information Security of the World Federation of Scientists, eds., 2011), http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf [https://perma.cc/BQ6Q-HJM3] (arguing that "unprovoked offensive cyber action, indeed any cyber attack, is incompatible with the tenets of cyber peace").

12 *See* Tapscott & Tapscott, *supra* note 8.

13 *See id*.

would designate a divine being as the trusted third party and in so doing finally grant security to the rapidly scaling global Internet.[14] A decade later, in the wake of the global financial crisis, an anonymous developer known as Satoshi Nakamoto "outlined a new protocol" that left divine intervention out the of equation. It leveraged peer-to-peer technology using distributed computation to create the cryptocurrency that would become known as Bitcoin.[15] This deceptively simple innovation "set off a spark that has excited, terrified, or otherwise captured the imagination of the computing world and has spread like wildfire."[16] Marc Anderssen, the co-creator of the first commercial browser, Netscape, has called the innovation "the distributed trust network that the Internet always needed and never had."[17] Enter the "Trust Protocol"—a technology authenticated "by mass collaboration and powered by collective self-interests, rather than by large corporations motivated by profit"—that has the potential to revolutionize business and cybersecurity across numerous contexts,[18] including critical infrastructure. Understanding the development of this technology, along with its potentials and pitfalls, is central to unpacking the promise of blockchains, and what—if any—regulatory steps need to be taken to ensure that they scale successfully.

This Article is structured as follows. Part 1 offers a technological and historical primer on blockchains featuring discussion of basic cryptographic principles and applications including Bitcoin and Ethereum, a smart contracts platform. Part 2 then focuses on applying blockchain technology to enhancing cybersecurity with a special emphasis on certificate authorities and critical infrastructure. Part 3 concludes the Article with an analysis of the benefits and drawbacks of regulating blockchain architecture and the promise of polycentric governance to help leverage blockchain technology to build trust and thereby promote cyber peace.

1. THE RISE OF BLOCKCHAIN AND BITCOIN: A TECHNOLOGICAL PRIMER

Despite its popularity, it could be said that Bitcoin has a "bad reputation" due in part to the extreme fluctuations in the crypto-currency's value, as well as some of the uses to which it is put (including extortion).[19] A case in point is the popularity

---

14 *See id*.
15 *Id*.
16 *Id*.
17 *Id*.
18 *Id*.
19 *The Trust Machine*, ECONOMIST (Oct. 31, 2015), http://www.economist.com/news/leaders/21677198-technology-behind-Bitcoin-

of demanding payment in Bitcoin for cybercriminal groups engaged in ransomware campaigns.[20] Yet at least some of this skepticism may, in fact, be misplaced. After all, the value of Bitcoin was largely stable for most of 2015 at approximately $250 before appreciating to an all-time high of more than $1,300 in March 2017,[21] while financial regulators have become more enthusiastic about the prospects of the crypto-currency; a case in point was the European Court of Justice's 2015 decision to recognize Bitcoin as a currency for purposes of avoiding Value Added Tax (VAT).[22] Perhaps the most often overlooked aspect of Bitcoin, though, is the blockchain technology underlying it, a technology that allows "people who have no particular confidence in each other [to] collaborate without having to go through a neutral central authority."[23] Simply put, according to *The Economist*, "it is a machine for creating trust,"[24] and trust is exactly what is needed if we are to secure certificate authorities and critical infrastructure from misuse, overuse, and abuse. First, though, before exploring the myriad applications that blockchains can have to improve cybersecurity, it is important to distinguish between Bitcoins and blockchains.

1.1 Analogizing Blockchains

To uncover the genius of blockchain technology, consider something mundane, like sending an email. When we do that (oftentimes far too frequent) task, what we are really doing is sending a copy of data, not the original.[25] We copy such information all the time, but we do not copy other things, like money. To do that, we rely on centralized institutions, institutions in which we have some degree of trust, like banks, governments, or even social media firms.[26] But relying on

---

could-transform-how-economy-works-trust-machine [https://perma.cc/Q5XT-EXX7].

20 *See, e.g.*, Mitchell Hyman, *Bitcoin ATM: A Criminal's Laundromat for Cleaning Money*, 27 ST. THOMAS L. REV. 296, 296 (2015).

21 *See, e.g.*, Jonathan Garber, *Bitcoin Super Spikes to an All-Time High*, BUS. INSIDER (Mar. 10, 2017, 9:05 AM), http://www.businessinsider.com/bitcoin-super-spikes-to-an-all-time-high-2017-3 [https://perma.cc/TVZ3-P5RX].

22 *See The Trust Machine*, *supra* note 19; Yessi Bello Perez, *Bitcoin is Exempt from VAT, Rules European Court of Justice*, COINDESK (Oct. 22, 2015, 9:58 BST) [https://perma.cc/J4KT-AXNW]; Pete Rizzo, *The Price of Bitcoin Just Jumped $30 in One Hour*, CODESK (Nov. 16, 2016, 13:30 BST), http://www.coindesk.com/price-Bitcoin-just-spiked-30-one-hour/ [https://perma.cc/SZQ9-YF7E].

23 *The Trust Machine*, *supra* note 19.

24 *Id.*

25 *See* Tapscott & Tapscott, *supra* note 1.

26 *See id.*

others to do such copying is not without its costs. We pay with money (think banking fees), and we pay with increased insecurity given the propensity for our information to be hacked, be it credit cards or health records.[27] Sometimes, we even have to pay with our privacy. Plus, such centralized systems can actually increase inequality given that up to two billion people around the world do not have bank accounts.[28] Enter the blockchain and one of its most popular applications to date, Bitcoin.

1.2 How Bitcoin Works

To the uninitiated, a helpful analogy to consider when seeking to understand Bitcoin is Napster, the early peer-to-peer file sharing service that first went online in 1999, which in turn inspired an entire industry of competitors.[29] Amongst its progeny are Skype and Spotify, as well as Bitcoin.[30] Bitcoin is not saved as a central file somewhere; instead, it is represented by blockchain transactions, a kind of "global spreadsheet" that leverages peer-to-peer technology to authenticate each transaction.[31] The transparency that comes with the blockchain being public is one of its greatest strengths.[32] Every 10 minutes, all new Bitcoin transactions are "verified, cleared, and stored in a block" that is, in turn "linked to the preceding block, creating a chain."[33] If these blocks do not refer to one another, then they are invalid; these blocks are also time stamped to further protect the blocks from being altered.[34] Similar to the reach of the World Wide Web, in time such blockchains can become a "World Wide Ledger of value."[35]

While Bitcoin involves a number of highly technical elements, it can be understood with little technical knowledge. The main point of Bitcoin is to replace physical currency by simulating a giant global ledger system. Each user has accounts with certain amounts of Bitcoins, as depicted in Figure 1.

---

27 *See id*.
28 *Id*.
29 Richard Nieva, *Ashes to ashes, peer to peer: An oral history of Napster*, FORTUNE.COM (Sept. 05, 2013) http://fortune.com/2013/09/05/ashes-to-ashes-peer-to-peer-an-oral-history-of-napster [https://perma.cc/V9HR-Y8TA].
30 *The Trust Machine*, *supra* note 19.
31 Tapscott & Tapscott, *supra* note 8.
32 *Id*.
33 *Id*.
34 *Id*.
35 *Id*.

Figure 1: A Traditional Ledger

Name	Balance
Alice	Ƀ10
Bob	Ƀ12
Carol	Ƀ13
Dave	Ƀ7

This process enables a system simulating cash by allowing transactions, which in turn update the ledger. For example, if Alice wishes to send Bob 5 Bitcoins (Ƀ), this can be accomplished by first checking that Alice has at least Ƀ5 in her ledger account and then implementing a transaction that decreases Alice's ledger by Ƀ5, and increases Bob's by Ƀ5. In principle, if there is a global ledger that can be easily updated in a secure and trusted manner, we can get rid of all physical currency (an attractive prospect to many businesses and investors in uncertain economic times)[36] and perform all transactions through ledger updates. Bitcoin provides a technological method to implement such a global ledger.[37]

It is also important to note that while it is conceptually simpler to think of a ledger as storing accounts with current balances, one can use another approach. For example, if instead of keeping a simple table as depicted in Figure 1, one can instead sum up the entire history of all transactions of an individual to determine their balance, as depicted in Figure 2. While impractical for a human in practice, it provides semantically the same information, and is simple for computers to process, even over very long transaction lists. It is this latter approach that Bitcoin supports.[38]

---

[36] *See Bitcoin Price Surges Beyond $675 Amid Brexit Vote*, CRYPTOCOINS NEWS (June 24, 2016), https://www.cryptocoinsnews.com/Bitcoin-price-surges-beyond-675-amid-brexit-vote/ [https://perma.cc/75GT-52UC].

[37] *See* Tapscott & Tapscott, *supra* note 8. One major feature that physical currency provides that seems to be absent from the above ledger scheme is anonymity. However, note that by simply using pseudonyms in the ledger scheme, where the mapping between individuals and pseudonyms is not known, then the ledger scheme can also provide anonymity.

[38] *See How Does Bitcoin Work*?, BITCOIN, https://Bitcoin.org/en/how-it-works [https://perma.cc/2JHP-GZAK].

Figure 2: A Transfer Ledger[39]

From	To	Transfer
…..	…..	…..
….	Alice	~~Ƀ~~10
…..	Bob	~~Ƀ~~12
…..	Dave	~~Ƀ~~3
Bob	Alice	~~Ƀ~~5
Alice	Dave	~~Ƀ~~7

Indeed, a proof of concept for how secure blockchain technology is, and its promise in promoting cybersecurity across a range of industries, lies in the story of Bitcoin itself. After all, proponents have claimed that "Despite an obvious prize and years to try, hackers have not cracked the prize. Bitcoin has been hacker proof to date. Contrast that history with most Global 2000 firms. No matter how big, no matter how much money they throw at cyber security, they get [h]acked. Regularly."[40] Though this claim has ultimately proven to be dubious given the proven instances of Bitcoin exchange hacks,[41] the underlying blockchain technology still boasts numerous cybersecurity advantages. To understand the promise (and peril) of this technology, though, a brief primer on distributed ledgers is in order.

1.2.1 A Distributed Ledger

At its root, a blockchain is a "shared, trusted, public ledger that everyone can inspect, but which no single user controls."[42] The participants in a given blockchain system work together to keep the ledger updated; it may be amended only by strict rules and consensus.[43] For example, Bitcoin's blockchain ledger "prevents double-spending and keeps track of transactions continuously," which is "what makes possible a

---

39 In Figure 2, new transactions are place on the bottom of the ledger. Assuming that this segment of the ledger shows all transactions that Alice, Bob, and Dave have ever been involved with, then after these transactions Alice has ~~Ƀ~~10+~~Ƀ~~5-~~Ƀ~~7=~~Ƀ~~8, Bob has ~~Ƀ~~12-~~Ƀ~~5=~~Ƀ~~7, and Dave has ~~Ƀ~~3+~~Ƀ~~7=~~Ƀ~~10.

40 Bernard Lunn, *Bitcoin Blockchain could Solve the Cyber Security Challenge for Banks*, DAILY FINTECH (Oct. 30, 2015), http://dailyfintech.com/2015/10/30/Bitcoin-blockchain-could-solve-the-cyber-security-challenge-for-banks/ [https://perma.cc/2SUB-9F3E].

41 *See, e.g.*, Yuji Nakamura, *The Wretched, Endless Cycle of Bitcoin Hacks*, BLOOMBERG TECH. (Aug. 17, 2016), https://www.bloomberg.com/news/articles/2016-08-17/the-wretched-endless-cycle-of-bitcoin-hacks [https://perma.cc/8EN6-KJ9K].

42 *The Trust Machine*, *supra* note 19.

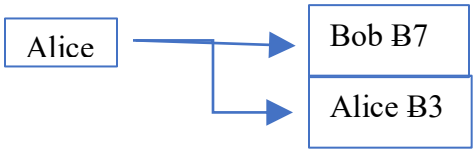
43 *Id.*

currency without a central bank."[44] It has also been said that blockchains are "the latest example of the unexpected fruits of cryptography."[45] To understand why, it is necessary to include a brief, non-technical excursion into cryptographic first principles. For those wishing such a background in cryptographic hash functions, digital certificates, and peer-to-peer networking, see Appendix A. For those with a sufficient understanding of these principles, we next turn to Bitcoin transactions.

1.2.2 A Primer on Bitcoin Transactions

Now that we have an understanding of some of the basic cryptographic tools used in blockchains, let us consider their application. To anchor ourselves to a concrete protocol we use the most famous, Bitcoin, and then discuss generalizations. Conceptually, the Bitcoin blockchain is nothing more than a global list of transactions that have been agreed upon via a form of consensus by a subset of the Bitcoin community. The transactions themselves are grouped into small lists called transaction blocks.[46] To understand these blocks, let us begin with a standard Bitcoin transaction, which transfers funds from one user, Alice from Figures 1 and 2, to another, Bob. We assume that Alice has Ƀ10 in her account. She wishes to perform a transaction, which simply means that she wishes to transfer some of the money in her account to another Bitcoin user, Bob. Say she needs to send Ƀ7 to Bob. This is accomplished by performing a send transaction that transfers *all* of the money in her accounts to new recipients. Alice must specify where this money is spent, as any money left off the table will be given as a transaction fee to Bitcoin miners, which will be described momentarily. Thus, Alice creates a transaction emptying her Ƀ10 account, sending Ƀ7 to Bob, and transferring the remaining Ƀ3 back to herself, visualized Figure 3.

Figure 3: Bitcoin Sample Transaction



The transaction itself is encoded as an appropriate binary bit-string by software and is sent onto the peer-to-peer (P2P)

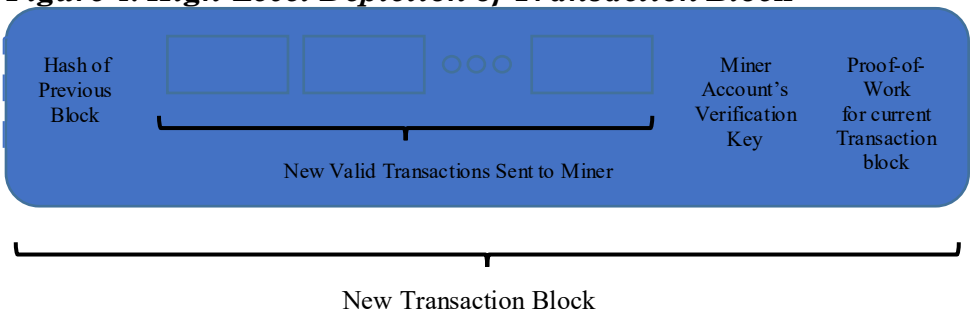
---

44 *Id.*
45 *Id.*
46 *See infra* Figure 4 and accompanying text.

network where it will be received by Bitcoin miners whose job it is to validate transactions. We put off discussion of Bitcoin miners for a moment to discuss several security issues that come up with the transaction as described.

First, recall that Alice's and Bob's accounts are virtual and that when the miners validate the transaction, all they do is agree that it is properly formed and thus legitimate. Consequently, there is not a single ledger space where Alice's balance is held, nor for Bob. Rather the ledger simulates the one in Figure 2. To determine Alice's balance, the miners go through all of Alice's prior transactions, determine the number of Bitcoins that have been given to her, and then subtract off all of the coins that she has spent. Anyone can do this, because every Bitcoin transaction that has ever been performed is stored publicly, by design, on the Bitcoin P2P network. While it may seem cumbersome, it is something that can be done at least somewhat efficiently by appropriately programmed computers, as is illustrated in Figure 4.

Figure 4: High-Level Depiction of Transaction Block



Let us now address the issue of how Bitcoin miners validate that a transaction is legitimate. The steps involved in this example include:

1) Ensuring that Alice, rather than a fraudulent party, created the transaction.
2) Ensuring that Alice has the Bitcoin necessary to fund the transaction.
3) Ensuring that there is no double spending.

We note that Alice's account name is not actually "Alice" or any other human readable string. Rather Alice's account name is a representation of the verification-key for a digital signature.[47] In practice, these are long strings of gibberish that represent large numbers.[48] For example, "1FCgBDLffB9NFVvuGK9YvVmnrB42hPDv9Q" might

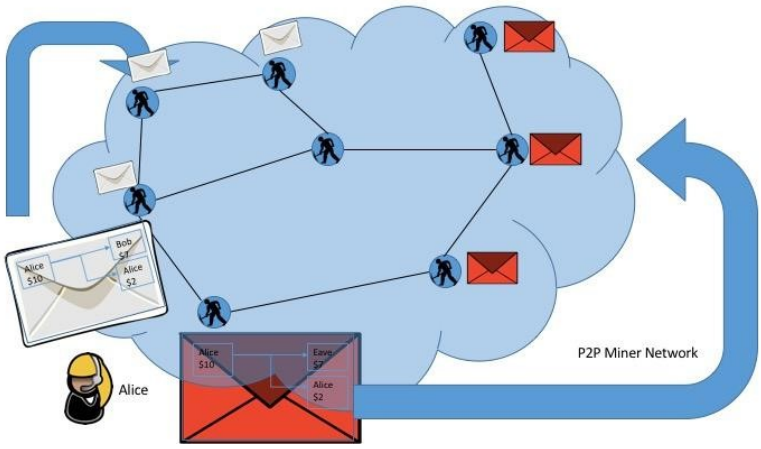
[47] *See infra* notes 275-76 and accompanying text.

[48] For more on this topic, see DIETER GOLLMANN, COMPUTER SECURITY 260 (2011).

represent one's verification key—in other words, their account. Anyone who wants to send Alice money sends it to her verification key, which she makes available as her account number to anyone who requests it. When Alice goes to spend money, she must sign her transaction with the account's corresponding signing-key, which only she knows and keeps private (as anyone who has access to her signing key can spend all of the money in her account). Since digital signatures are unforgeable, when a transaction looking to spend the money in a given account comes in, it is first checked for a valid digital signature; if the signature verification fails, then the transaction is discarded as illegitimate. If, on the other hand, the signature is valid, we know that it was sent by someone who has the corresponding signing key, and thus technically has spending authority.

For the second goal of ensuring that Alice has sufficient funds, a miner goes through the history of transactions that involve Alice and takes the difference between credits and debits to her account name, thus determining her balance. However, since there are many miners on a distributed P2P network, it is possible that Alice sent four different miners transactions—such as sending Ƀ7 each to Bob, Carol, Dave, and Eve, in each case sending the remaining Ƀ3 back to herself. If each miner accepted the transactions as legitimate and put them on the transaction list, then from an initial Ƀ10, Alice is able pay out Ƀ28 cumulatively and end up with Ƀ12 in change. This double spending illustrated in Figure 5 leads to our third security goal.[49]

Figure 5: Double Spending in P2P Networks



In order to ensure that individuals do not double spend,

[49] For more on double spending, see PEDRO FRANCO, UNDERSTANDING BITCOIN: CRYPTOGRAPHY, ENGINEERING AND ECONOMICS 163 (2014).

we need to ensure that there is *consensus* about the transactions that should be considered part of the transaction history. Because potentially many different organizations process transactions on the P2P network, the double-spending problem above requires consensus between relevant parties. Further, since any party can become a miner, there is no guarantee that they are fair actors, and so we need to ensure the veracity of consensus even in the presence of bad-actors. Finally, the transaction must have distributed coordination, as by design Bitcoin rejects any central coordinate that could become a point of security failure.

Blockchains, the subject of this article, pose a solution. This introduces us to the most important role that miners play. In essence, miners provide consensus for the blockchain. They do this through the following five steps:

1) taking as input the transactions individuals send them;
2) verifying transactions for syntactic correctness, valid signatures, and sufficient funds;
3) pooling correct transactions into a transaction block;
4) performing a proof-of-work to legitimize the transaction block; and
5) broadcasting the results to the community.[50]

Steps one and two are straightforward and have been discussed previously. Transaction blocks in *step three* are a new concept, but are relatively straightforward; when a miner receives a transaction that is correct and passes all necessary checks, it is automatically added to the block.[51] The block, in turn, is simply an amalgamation of transactions that have not been included in the official record of approved transactions by being linked to the previously accepted transaction blocks.[52] Each of the transaction blocks point, via a reference, to the previous transaction block. This forms a chain of transaction blocks (e.g., a blockchain), and following this chain to the original block terminates in the Bitcoin genesis block.[53] This is the first block of Bitcoin transactions, and the fact that the chain points to this specific block is what distinguishes true Bitcoins from any other group of people taking the same technology, running it, and producing an alternate competing currency.[54] In fact, Bitcoin developers run several alternate networks, featuring alternate genesis blocks, to allow for testing and development

---

50 *See, e.g.*, ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES 174-199 (2014).

51 *See* MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY at x, 3-5 (2015).

52 *See supra* Figure 4.

53 *See* ANTONOPOULOS, *supra* note 50, at 164.

54 *See id*.

without affecting the actual Bitcoin blockchain.[55]

The question underlying *step four* then becomes how one decides which transaction block to add to the official transaction block history list. The answer is that the first miner to present a valid proof-of-work on the transaction will have it added to the end of the block-chain.[56] Miners are asked to perform a proof-of-work on a transaction block in order for it to be added. A proof-of-work is 'memoryless,' that is, it is a probabilistic process, and previous failures do not increase the odds of future success.[57] This is important, as there is little disincentive to accept new transactions and add them to a transaction block while searching for a proof-of-work—adding a transaction does not discard previous work done.[58] The first miner to provide such a proof updates the chain. Proofs-of-work are set at a difficulty level such that it is fairly unlikely that multiple miners will find proofs-of-work for their respective blocks at the same time, or close to the same time.[59]

When a miner finds a valid proof-of-work for its transaction, it announces it on the P2P network circa *step five*.[60] All miners who receive the new transaction will check it for validity, that the proof-of-work is complete, and that it attaches to the end of the current transaction chain.[61] Assuming it does, then the miners will accept this as the new end of the blockchain. The miners then update their current transaction blocks, remove any transaction in the block they are currently working on that are now inconsistent (e.g., transactions that have already been approved, or transactions that involve doubly spending coins with approved transactions), and point their transaction block at the new end of the chain.[62] However, if a miner receives a completed transaction block that does not point to the end of the current blockchain as the miner knows it, but which is otherwise valid

---

55 *See supra* note 51 and accompanying text. Note that because of the P2P nature of the underlying communication network, it is likely that at any given time different miners will have different transactions in their current transaction block. Each transaction block should locally be consistent with all the previous transactions in previous transaction blocks, but different miners' transaction blocks might be globally inconsistent (for example, if people are trying to double spend). *Id.*

56 *See infra* note 271-73 and accompanying text.

57 *See* ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION 43 (2016).

58 *See id.*

59 Michael Nielsen, *How the Bitcoin Protocol Actually Works*, DATA-DRIVEN INTELLIGENCE BLOG (Dec. 06, 2013) http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/ [https://perma.cc/Z968-2LAP].

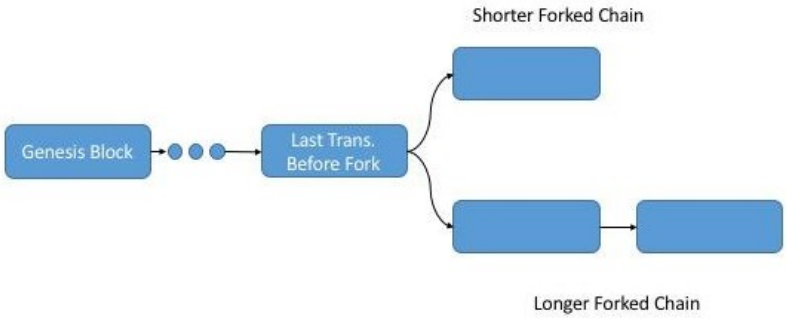
60 *See* NARAYANAN ET AL., *supra* note 57, at 131.

61 *See* Nielsen, *supra* note 59.

62 *Id.*

(that is, it points back to the genesis block, and is constituted by valid blocks throughout), then the blockchain is said to be split, or "forked."[63] The miner must then make a decision about which chain it will connect to its current transaction block. The best answer is for the miner to choose the longest blockchain (the one with the most transaction blocks) since this represents the larger computational effort, and thus the support of the majority of the community. Although such forks can happen for technical reasons, they can also result from regulatory interventions such as different jurisdictions taking varied approaches to blockchain management, a topic discussed further in Part 3.[64]

Figure 6: A Fork in the Blockchain[65]



In order to ensure that finding successful proofs-of-work for block-chains does not become too frequent—making forking a more likely process—the blockchain protocol has a natural moderating principle built in. The difficulties of the proofs-of-work used in the blockchains are adaptively changed to make

63 NARAYANAN ET AL., *supra* note 57, at 172.

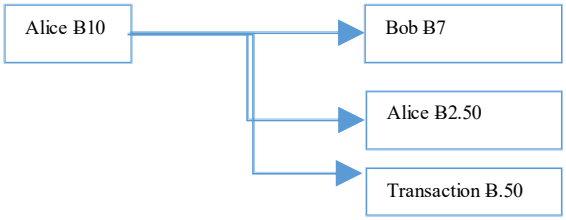
64 *See infra* Section 3.3.

65 Two different chains extend from a given transaction block. The network now must decide which of these forks is legitimate to arrive at shared consensus. Not shown in Figure 6 is what happens in the case of a tie, or near tie (e.g., two blockchains of similar or equal length). In such an outcome, the miner must choose one chain to follow. Although the community will only accept the longest chain, because of communication delays and other problems it is possible for there to be several competing chains that simultaneously are essentially the same length. Eventually, through random processes, one will become substantially larger than the other, and the community will coalesce around this chain. All transaction blocks in the dropped fork are now invalid, and ignored. Any transactions that were only approved in the deprecated chain are now null and void. *See, e.g.*, Vitalik Buterin, *Bitcoin Network Shaken by Blockchain Fork*, BITCOIN MAG. (Mar. 13, 2013, 11:14 PM EST), https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/ [http://perma.cc/2XHQ-7NXE]. When non-technical means result in a fork, it is uncommon for blockchain forks to vary in length by more than one block. Thus, participants in a transaction are typically cautioned to ensure that at least three transaction blocks are confirmed as part of the blockchain after the one including their transaction of interest. This ensures it is highly likely that their transaction is not involved in a fork of the blockchain that will eventually be discarded.

the amount of time they take to solve relatively constant and predictable, regardless of the computational power available to the miners. That is, difficulties are made easier or harder to ensure that they take, on average, ten minutes for anyone on the network to come up with a valid proof-of-work.[66]

Given that anyone can become a miner in this decentralized, voluntary system, a question that naturally arises is: what motivates the miners? Simply put, they are paid. This is done through two methods. By design, currently the Bitcoin network pays any successful miner a fee each time the miner has a successful proof-of-work for a transaction-block that gets placed into the blockchain.[67] The second is through transaction fees. During a transaction, the payer has the option of specifying an amount that goes to the miner, as shown in Figure 7.

Figure 7: Bitcoin Transaction Fees



The miner includes their own verification key in the transaction block, and upon finding a proof-of-work, all transaction fees in the block are assumed to be added to that account. Based on how many blocks are between the confirmed block and the transaction block (e.g., which block has the corresponding proof attached) miners are paid a specific rate. Initially, miners were paid Ƀ50 for each successful proof-of work. However, the system is built so that for every 210,000 transaction blocks that are added to the chain, the value paid is decreased by half.[68] Importantly, these are not Bitcoins that

---

66 NARAYANAN ET AL., *supra* note 57, at 108. This is done by dynamically adjusting the difficulty of the proof-of-work that is expected for a block to be added to the chain, based on how long it has taken on average to solve previous ones in a sliding window of time. The time involved is relevant to computing power and energy use. By some estimates, Bitcoin mining could consume as much energy as Denmark by 2020. *See* Sebastiaan Deetman, *Bitcoin Could Consume as Much Electricity as Denmark by 2020*, MOTHERBOARD (Mar. 29, 2016, 11:30 AM), http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020 [http://perma.cc/C7XB-367B].

67 *See How Bitcoin Mining Works*, COINDESK.COM http://www.coindesk.com/information/how-bitcoin-mining-works/ [https://perma.cc/JAB3-ED7M].

68 Since there is a minimal fractional currency in the Bitcoin system, this halving function implies that there eventually will be no direct payment for

are transferred from another Bitcoin user, but rather are spontaneously created in the system, which is the only process by which new Bitcoins are created in the system. It is also where the term "miner" comes from, as they mine (by doing proofs-of-work) looking for digital gold (Bitcoins). A corollary is that there is a fixed number of Bitcoins that can be created under the current system, meaning that Bitcoin will eventually be an inherently deflationary currency.

1.2.3 Anonymity

Since Bitcoin wishes to duplicate physical currency, it needs to maintain one of its crucial property: anonymity. In order to accomplish this, the system must account for two important issues. First, note that one's account on the Bitcoin network does not need to be created or verified by a central identity, which is one reason for its popularity in cybercrime syndicates.[69] Individuals can and do create their own digital signing key-pairs on local computers, and the verification key is the account number. There is no central authority where verification keys are vetted or correlated with physical identities.[70] The security properties of digital signatures ensure that it is a statistical impossibility that two people end up with the same verification key, and thus there is no concern for collisions where multiple individuals generate the same key and thus share the account. Further, there is essentially no cost in generating new verification keys, so people can—and do—generate multiple accounts and verifications keys.[71] Some go so far as to generate a new set of keys for each transaction,[72] and take countermeasures to mask their Internet Protocol (IP) addresses so that their transactions cannot be traced.[73]

---

miners, and all motivation for miners will come in the form of transaction fees. NARAYANAN ET AL., *supra* note 57, at 65.

69 *See* RYAN KO & KIM-KWANG RAYMOND CHOO, THE CLOUD SECURITY ECOSYSTEM: TECHNICAL, LEGAL, BUSINESS AND MANAGEMENT ISSUES 52-53 (2015); NARAYANAN ET AL., *supra* note 57, at 138;.

70 *See* NARAYANAN ET AL., *supra* note 57, at 1.

71 *Id*. at 56.

72 *See id*.

73 In order to maintain the verification key's anonymity, it is important to prevent the key from being linked to an identity. This precludes users from sharing keys broadly, and from directly linking them to their identities. However, this also means that users need to take precautions when making transactions, as the communication channel itself might be used to establish a connection between the identity of the user and the verification key of the transaction. For example, a user who uses a verification key *vk*, and connects directly to the P2P network with no countermeasures, is likely to have their connecting IP address (e.g., 1.2.3.4) logged into the contacted P2P system's audit-logs. Those can later be correlated with the reception of the transaction, and thus the verification key may be tagged to a user's IP address. If the IP address is static or otherwise identifies a small number of users or systems,

However, even with these precautions, the blockchain technology undergirding Bitcoin is vulnerable to cyberattacks, as is discussed next.

1.2.4 Computational Attacks on Blockchains

One of the key values of blockchains is that they represent an immutable public-ledger that is arrived at by distributed consensus. However, as we saw in Section 1.2.2, there are times when the blockchain can fork, and where there are multiple possible ways the blockchain might resolve itself. It was for this reason that users were advised to wait for three transaction blocks to have valid proofs-of-work before viewing the transaction as accepted. However, it may have occurred to the observant reader that there is no technical countermeasure preventing an adversary from attempting to insert their own fork into blockchains and thereby delete some transactions (e.g., those that occur after the fork on the original chain).[74] An attacker can do this by starting to provide new transaction blocks with valid proofs-of-work that link back to an arbitrary transaction block in the blockchain, as opposed to the end of the chain. If they can make this fork longer than the current valid chain, they can—in theory—convince other miners to accept their new fork. Let us consider this attack from two perspectives, technical and social, before discussing its application to blockchain cybersecurity in the certificate-authorities and critical-infrastructure contexts.

1.2.4.1 Technical

In order to produce new proofs-of-work for a large number of transaction blocks, an adversary will need to control a high percentage of computational power. Specifically, they will need enough power to produce proofs-of-work at a pace

---

this may de-anonymize the owner of the verification key, or at the very least narrow the list of possible candidates. Therefore, a user who cares about anonymity might use publicly available access points or the Tor network to mask their connecting IP. *Cf.* Wendy McElroy, *Bitcoiners Who Use Tor—Be Warned!*, BITCOIN.COM (Aug. 26, 2016), http://news.bitcoin.com/update-bitcoiners-use-tor-warned/ [http://perma.cc/TWJ2-3PCJ]. However, many who do not care about anonymity, such as merchants, publish their verification keys. *See, e.g.*, *How Can I Generate API Keys for My Merchant Account?*, COINBASE (Aug. 22, 2016), http://support.coinbase.com/customer/portal/articles/1914910-how-can-i-generate-api-keys-for-my-merchant-account [http://perma.cc/A3MG-FUMM].

74 *See, e.g.*, Alyssa Hertig, *The Blockchain Created by Ethereum's Fork is Forking Now*, COINDESK (Oct. 25, 2016, 4:23 AM BST), http://www.coindesk.com/ethereum-classic-blockchain-fork-ddos-attacks/ [http://perma.cc/M8CT-GXPU].

that is faster than the rest of the network combined. They need to produce proofs-of-work on new transaction blocks on their forged chain until its length is longer than the currently accepted valid tail of the fork. Being able to produce transaction blocks at a pace that is faster than the rest of the mining network, in turn, implies that the adversary needs to have more computational power than the rest of the network. Thus, once any miner controls more than fifty percent of the processing power of the mining network, it can in principle dictate the transactions accepted into the ledger.[75] This allows it to act as a gatekeeper on transactions, which could have catastrophic consequences given that such an adversary could pick and choose transactions it liked out of the original blockchain, and include them in its new forked chain.[76] Even if a small number of miners controls greater than fifty percent of the computational power, this poses the risk that they may form an oligarchy. Historically, there is precedent for miners policing themselves to ensure that there is diversity in the concentration of the computational power of the network.[77] In practice, though, there is more concern that an individual or small group that controls more than fifty percent of the computational power will be able to modify the recent history of the blockchain as opposed to previous arbitrary points due to social aspects, as discussed next.

1.2.4.2 Social

Any attempt to modify a large history of the blockchain is likely to run into non-technical issues. Namely, the miners are still individuals and groups with social norms and expectations, which are discussed further in Part 3. Thus, while typical miners operate automated systems that automatically validate transactions based on algorithmic rules, they can and will make exceptions. For example, should all of the miners be flooded with a new tail to the blockchain that invalidated large numbers of previous blocks, causing a fork, then there would be significant social pressure to ignore this fork in the blockchain. Because many of the miners would lose the financial rewards (both transaction fees and mined coins) for their efforts in previous mining, not to mention the consumers and merchants who would object to their previous transactions being invalidated, miners could socially agree to

---

75 *See, e.g.*, Fran Berkman, *What Is a 51 Percent Attack, and Why Are Bitcoin Users Freaking out About it Now?*, DAILY DOT (Feb. 24, 2017, 7:26 PM), http://www.dailydot.com/business/bitcoin-51-percent-attack/ [http://perma.cc/YDG3-VJYE].

76 *See id*.

77 *See id*.

manually prevent the specified fork from being added. Yet, in a scenario where everyone agreed to ignore such a fork (or transaction block), actors might still worry unless the mining network was confident that it had, at that point, increased its mining power such that it again represented more than fifty percent of the computing power—or the problem might very well repeat itself. Already, there has been at least one occasion where a blockchain community has largely agreed through social mechanisms to ignore a given fork or transaction block.[78]

1.3 Viewing Blockchains as Computational Engines

While blockchains have now been explained in the context of basic Bitcoin transactions, it is worth discussing the fact that blockchains are capable of generalizing to perform more complicated tasks than the simple transactions already explained. In fact, the programming language Script allows one to engineer more complicated transactions, such as those that require multiple people to sign off on a transaction, or require a transaction to only be valid if certain conditions are met.[79] In practice, a common requirement is for multiple signatures to be required for a Bitcoin to be spent, adding a check against theft and fraudulent spending.[80] In theory, more complicated contracts are possible, too, although not all of the Script language is fully supported by most miners, making it less clear which contracts can be supported. For example, in theory, Alice can make a transaction whereby she pays Bob some number of Bitcoins on the condition that Charlie pays Alice. Alice can send this transaction directly to Bob who can then hold it until he sees a payment from Charlie to Alice materialize on the blockchain. At that point, Bob can submit Alice's previously created transaction to the miners for validation.

In any event, the fact that transactions can easily be shown to be more complicated allows us to see that the blockchain is duplicating a distributed computation. One can imagine everyone's accounts as the base state, and a transaction that moves value from one account to others as a state modifying transition function. Those familiar with computing will realize that this represents a computational device. Here, the power of the computational device is dependent on the complexity of the transition functions that can be written. Bitcoin has purposefully limited the complexity of the transactions that can be created to prevent certain

---

78 *See id*.
79 *See* FRANCO, *supra* note 49, at 91.
80 *See id*.

attacks on the system, but the concept is clear—blockchains can, in theory, become distributed computers that can handle any computation a regular computer would (although potentially much more slowly). This leaves open the possibility for many other uses of blockchains, such as using them to encode small programs that move assets around—in less technical terms, providing a platform for smart contracts.

Indeed, as with blockchain technology generally, the myriad applications that this technology affords have received unsatisfactory attention in the legal literature to date.[81] That omission is somewhat surprising given the claims by new market entrants such as Ehtereum, which is a startup blockchain platform provider through which "anyone can set up a node that validates, observes and submits transactions."[82] This technology intersects with the law insofar as Ethereum users can use the platform to "create arbitrary contracts which can be used in a permisionless or permissioned group of users," contracts that can also make use of the digital "Ether" currency to theoretically make enforcement automatic.[83] Yet Ethereum also has its critics,[84] opening the door for new entrants and cybersecurity applications, some of which are discussed next in Part 2.

2. APPLYING BLOCKCHAIN TECHNOLOGY TO ENHANCE CYBERSECURITY

Myriad methods and business plans have been created to leverage the promise of blockchain technology to build trust and enhance cybersecurity across systems, networks, and sectors. Even Walmart is experimenting with the technology to enhance food safety.[85] As noted above, though, this is a movement that has largely been ignored by the legal literature. Although a comprehensive review of the state of play in this

---

81 *See* Isaac Pflaum & Emmeline Hateley, *A Bit of a Problem: National and Extraterritorial Regulation of Virtual Currency in the Age of Financial Disintermediation*, 45 GEO. J. INT'L L. 1169, 1180 n.47 (2014) (collecting sources on the expansion of blockchain technology beyond money).

82 Marin Bartlam & Mikaela Kantor, *Can Blockchain Live up to the Hype?*, JDSUPRA (July 28, 2016), http://www.jdsupra.com/legalnews/can-blockchain-live-up-to-the-hype-57369/ [http://perma.cc/YY5P-ZP35].

83 *Id*.

84 *See, e.g.*, Jon Reed, *Building Blockchain Apps for the Enterprise—a Q/A with Victor Wong*, DIGINOMICA (June 28, 2016), http://diginomica.com/2016/06/28/building-blockchain-apps-for-the-enterprise-a-qa-with-victor-wong/ [http://perma.cc/N2E5-NZ9W] (interviewing a company represeneative who "provides the tools to develop apps on Ethereum[.]").

85 *See* Jon Fingas, *Walmart Tries Using Blockchain To Take Unsafe Food off Shelves*, ENGADGET (Nov. 21, 2016), http://www.engadget.com/2016/11/20/walmart-uses-blockchain-for-food-safety/ [http://perma.cc/F25T-G9LL].

burgeoning field is beyond the scope of this Article, we offer a snapshot to help provide some context and then dive into a case study unpacking the promise of using blockchains to secure certificate authorities in an effort to enhance the cybersecurity of critical infrastructure.

2.1 Blockchains and Cybersecurity

Examples abound regarding how firms are using blockchains to enhance cybersecurity; after all, at its most basic level, it is an open-source code that can be downloaded and run by anyone for free.[86] Due to these exceedingly low barriers to entry, this technology has the potential to unleash 'coinless' cybersecurity applications. Already, Marc Andreessen, a venture capitalist, has invested more than fifty million dollars in blockchain technologies.[87]

At its root, blockchains allow industries, and the Internet more generally, to return "to a decentralized Internet . . . [but this] will only happen when it becomes accepted that decentralized is safer than centralized."[88] The issue, or so its proponents maintain, is maximizing distribution in a cybersecurity era in large part defined by centralization.[89] To the finance industry in particular, accustomed to building walls and safes, this change in mindset to decentralization can be a difficult sale. But if the sale is made, then banks in particular could have the benefit in ways ranging from reduced server and personnel costs to better informed decision-making.[90]

Indeed, while Bitcoin may be described as "a brilliant solution looking for a problem to solve,"[91] the underlying technology of blockchains have immediate applicability across myriad industries and sectors that could help better address the multi-faceted cyber threat facing the finance industry, a threat that has even been called "systemic."[92] The tamper-proof power of blockchains—so long as no single entity controls more than fifty- percent of the computing power on the network—is also powerful given the extent to which the cryptographic principles introduced in Part 1, which are designed for information security, are also "paradoxically, . . . a tool for open

---

86 Tapscott & Tapscott, *supra* note 8.

87 Misha Tsukerman, *The Block is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future*, 30 BERKELEY TECH. L.J. 1127, 1144 (2015).

88 *See* Lunn, *supra* note 40.

89 *Id.*

90 *See id.*

91 *Id.*

92 *Id.*

dealing."[93] Indeed, the bonanza could be so great that some startups are already working on small-scale blockchain search engines, a task made easier given the fact that "blockchain enables radical transparency a lot easier than it enables radical anonymity."[94] Although no blockchain has yet scaled to the extent necessary to search the entire Web, theoretically such engines enjoy the benefit of being able to search not only at one point in time, but also over time, meaning that blockchains could "add the additional dimension of time" more easily to queries.[95] For example, it is possible to research the first Bitcoin transactions, to trace an individual coin back to the first time it changed hands—famously, in the case of Bitcoin, that was a pizza order costing 10,000 Bitcoins, which as of November 2016 would be worth more than $7 million.[96] One day, recruiters may even be able to search for applications from a publicly available blockchain featuring the relevant qualifications, and potentially foregoing extraneous information (such as age, sex, or national origin), and, for that matter, serendipity.[97] Similar outcomes could be in the works for the multi-billion dollar Internet marketing industry; in short, "you'll be paying customers to listen to your elevator pitch, but you will have tailored your query to pitch only to a sharply defined audience so that you will be reaching exactly the people you want to reach without invading their privacy," an idea called "*black box marketing*."[98]

One application that is gaining some traction, for example, is to create secure public databases, such as for land registries with countries such as Honduras and Greece already expressing interest.[99] The same can be done for the ownership of anything valuable, from rare artworks to luxury goods to

---

93 *The Trust Machine*, *supra* note 19; Theodore Kinni, *Tech Savvy: How Blockchains Could Transform Management,* MIT SLOAN MAN. REV. (May 12, 2016), http://sloanreview.mit.edu/article/tech-savvy-how-blockchains-could-transform-management [https://perma.cc/VG9V-DAMZ] ("Now imagine the opportunities that arise from the ability to search the World Wide Ledger, a decentralized database of much of the world's structured information. Who sold which discovery to whom? At what price? Who owns this intellectual property? Who is qualified to handle this project? What medical skills does our hospital have on staff? Who performed what type of surgery with what outcomes? How many carbon credits has this company saved? Which suppliers have experience in China? What subcontractors delivered on time and on budget according to their smart contracts? The results of these queries won't be resumes, advertising links, or other pushed content; they'll be transaction histories, proven track records of individuals and enterprises, ranked perhaps by reputation score.").

94 *Id.*.

95 *Id.*

96 *Id.*

97 *Id.*

98 *Id.*

99 *The Trust Machine*, *supra* note 19.

securities.[100] In many ways, blockchains can fulfill the function of a notary (or as discussed below, a certificate authority), and be applied in any context in which trust is essential; which, in this day and age, is most of the time. In such scenarios, miners' incentives are defined by the application in question, but can often be covered by transaction fees. Thus, just as now, when one pays transaction fees for purchasing land, or luxury goods, part (or all) of that fee would be used to incentivize miners on a blockchain to process and record the transaction. It is worth noting that in these scenarios no "coins" need to be produced.

Indeed, financial firms are amongst those most enthralled by the power of blockchain technology given the fact that this would relieve them from having to have a private, centralized (and hence vulnerable) internal ledger for which each transaction must be checked against the records of a counterparty.[101] Some estimates place the total amount that this could save the banking industry at roughly $20 billion by 2022; in fact, twenty-five banking firms have already joined a blockchain startup called R3 CEV to develop common standards and further catalyze the industry.[102] NASDAQ has also announced its intention to begin trading the securities of private firms using blockchains.[103] Yet some of the greatest potential for this technology may lie in its ability to mitigate an ongoing threat to the Internet generally, and critical infrastructure in particular—strengthening certificate authorities.[104] It is to that topic that we turn to next.

2.2 The Insecurity of Certificate Authorities

Certificate authorities are third parties that companies and website owners use to identify individuals or organizations and tie their identities to public cryptographic keys.[105] This allows users that trust the certificate authority to later trust that an arbitrary public key received over the Internet (or some other communication channel) belongs to the appropriate party, and therefore messages from it correspond to the identity indicated by the certificate authority (CA).[106] As a

---

100 *Id.*
101 *Id.*
102 *Id.*
103 *Id.*
104 *See, e.g.*, Peter Loshin, *Mozilla to Drop WoSign as a Trusted Certificate Authority*, TECHTARGET (Sept. 29, 2016), http://searchsecurity.techtarget.com/news/450400087/Mozilla-to-drop-WoSign-as-a-trusted-certificate-authority [https://perma.cc/7MYZ-R3BC].
105 *See, e.g.*, DERRICK ROUNTREE, SECURITY FOR MICROSOFT WINDOWS SYSTEM ADMINISTRATORS 38 (2011).
106 *See id.*

rough metaphor, if one received a text message from an unknown number asking you to send it some confidential information on an upcoming business transaction with the person claiming that they are a known and eligible recipient of said information, you would be rightly hesitant to send the requested data.[107] However, if a trusted confidant (acting in the role of the certificate authority) assured you that the unknown number corresponds to the individual in question, you would be more likely to comply and send the information. The metaphor breaks down, though, because one never meets a CA in the real world; rather, your computing infrastructure is built trusting a large number of them by default. In fact, the typical browser will trust hundreds of CAs from around the world, with some of that trust being misplaced, opening the door to cyber attacks.[108]

Unfortunately, due to reasons varying from simple mishaps to clandestine government intervention, certificate authorities are sometimes not themselves trustworthy.[109] Firms, including Google and Mozilla, have implicitly trusted these certificate authorities even though they can lie about users' identities or be hacked, resulting in an attacker obtaining false certificates.[110] For example, in early 2011, nearly 200 different certificate authorities fulfilled Mozilla policies and thus could be used to find websites on Firefox, including the China Internet Network Information Center (CNNIC), which is run by the Chinese government.[111] In mid-2011, fraudulent certificates were obtained from the servers of Comodo, a popular certificate authority that creates certificates for the likes of Gmail and Yahoo! Mail, allegedly by an Iranian hacker.[112] But these attacks are just the tip of the iceberg. The

---

107 *Cf.* Rees Johnson, *Techniques, Lures, and Tactics to Counter Social Engineering Attacks*, DARK READING (Mar. 9, 2015), http://www.darkreading.com/partner-perspectives/intel/techniques-lures-and-tactics-to-counter-social-engineering-attacks-/a/d-id/1319401 [https://perma.cc/PH76-6X29].

108 *See, e.g.*, Richard Chirgwin, *Google Publishes List of Certificate Authorities it Doesn't Trust*, REGISTER (Mar. 23, 2016), http://www.theregister.co.uk/2016/03/23/google_now_publishing_a_list_of_cas_it_doesnt_trust/ [https://perma.cc/5Q92-EZX3].

109 Interview with Chris Palmer, Google engineer and former technology director, Electronic Frontiers Foundation, in San Francisco, Cal. (Feb. 25, 2011).

110 *See, e.g.*, Danny O'Brien, *The Internet's Secret Back Door*, SLATE (Aug. 27, 2010), http:□□www.slate.com□articles□technology□webhead□2010□08□the_internets_secret_back_door.html [https://perma.cc/GL3N-SWC6] (reporting on the vulnerabilities created by these certificate authorities).

111 *See Add China Internet Network Information Center (CNNIC) CA Root Certificate*, Bugzilla@Mozilla, https:□□bugzilla.mozilla.org□ [https://perma.cc/2VCE-2R2G]; *Mozilla Included CA Certificate List*, MOZILLA, http://www.mozilla.org/projects/security/certs/included/ [https://perma.cc/D3AK-6UGK] (last visited Nov. 12, 2013).

112 *See* Peter Bright, *Another Fraudulent Certificate Raises the Same Old*

Stuxnet attack was enabled, at least partially, by certificate authorities in Taiwan that signed off improperly on identities, which is believed to have been caused by clandestine government interference.[113] Beyond the business context, the vulnerabilities in certificate authorities hold the promise of making critical infrastructure less secure. This is because an increasing amount of critical infrastructure is being connected to the Internet, opening the door to blockchain applications to improve security.[114]

2.3 Leveraging Blockchains to Enhance the Security of Certificate Authorities

One of the problems with current Certificate Authorities is that ultimately the issuances of certificates that bind real world identities to digital signing keys involves people. Therefore, whether due to untrustworthiness, malfeasance, incompetence, or some combination thereof, certificates get issued that improperly bind identities to keys. For example, certificate authorities in Turkey have issued certificates that bind Google's identity to keys that do not correspond to it, allowing users to connect to sites that they believed were Google, but were in fact a third party.[115] In theory, an individual can check which CA signed the certificate in question, and then verify for unusual or changed CA's (in fact, this is how the issue with the Turkey issuance was eventually made public),[116] but even most security experts do not take the effort to check for such changes due to time and resource constraints.[117] Perhaps unsurprisingly then, the fake issuance of Google's certificate is not an isolated case, but similar issues

---

Questions About Certificate Authorities, ARSTECHNICA (Aug. 29, 2011), http:□□arstechnica.com□security□2011□ 08□earlier-this-year-an-iranian [https://perma.cc/QH9H-FPQC]; Ms. Smith, *Chrome, Firefox, IE to Block Fraudulent Digital Certificate*, NETWORKWORLD (Jan. 4, 2013), http://www.networkworld.com/community/blog/chrome-firefox-ie-block-fraudulent-digital-certificate [https://perma.cc/YEN9-UKVJ].

113 *See* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1032 (2014).

114 *See* Taylor Armeding, *How Much at Risk is the U.S.'s Critical Infrastructure?*, CSO (Jan. 21, 2016), http://www.csoonline.com/article/3024873/security/how-much-at-risk-is-the-uss-critical-infrastructure.html [https://perma.cc/Q664-95XG].

115 Sean Gallagher, *Turkish Government Agency Spoofed Google Certificate "Accidentally*," ARSTECHNICA (Jan. 4, 2013), http://arstechnica.com/security/2013/01/turkish-government-agency-spoofed-google-certificate-accidentally [https://perma.cc/WY4B-HEK8].

116 *See id*.

117 *See, e.g.*, *How Cybercrime Exploits Digital Certificates*, INFOSEC INST., http://resources.infosecinstitute.com/cybercrime-exploits-digital-certificates/ [https://perma.cc/4TLV-XXFZ] (last visited Nov. 21, 2016).

have plagued Microsoft[118] and many other firms.[119] In some cases, CA's had so many issues with properly issuing certificates that software companies have refused to recognize any certificate they issue.[120]

Blockchains provide a technology to circumvent the problems of accidental issuance exactly because they represent a large immutable public ledger. The goal now is to insert users' and organizations' certificates into the public ledger, rather than relying on potentially nefarious third parties. The non-malleability and public nature of blockchains allow one to publicly post their certificates without the need for validation by a CA.[121] Moreover, certificates can be long-lived on the blockchain, meaning that the issuance of new certificates for the same organization on the blockchain can be questioned and subject to specific criteria to ensure the risk of its use is minimal.[122] When a certificate user trusts that a given certificate is legitimate, it can invest computational effort as a miner to add weight that the certificate is indeed legitimate. For example, every time a user makes a connection to Amazon using an encrypted channel through their browser, they can expend some computational effort to validate Amazon's certificate, and have this recorded in the blockchain. Frequently used, and long lived certificates will be viewed as more trusted than newly issued certs that are infrequently used. This is because there would be significantly more proofs-of-work for such long-lived, well used certificates, than for newly issued ones. However, this makes it difficult for well-established brands to produce new high-confidence certificates when needed, as they will have to develop their own history. Some ability to transitively share trust across certificates may allow one to rectify this problem.

Similarly, users can be warned that the identity is

---

118 Lucian Constantin, *Microsoft Revokes Trust in Certificate Authority Operated by the Indian Government*, PC WORLD (July 11, 2014), http://www.pcworld.com/article/2453343/microsoft-revokes-trust-in-certificate-authority-operated-by-the-indian-government.html [https://perma.cc/D5A2-2CQN].

119 Chris Paoli, *Microsoft Issues Advisory to Block Spoofed Google and Yahoo SSL Certs*, REDMOND MAG. (July 11, 2014), http://redmondmag.com/articles/2014/07/10/block-spoofed-ssl-certs.aspx [https://perma.cc/53K2-HBEV].

120 Dominique Rafael, *Firefox to Block Chinese Certificate Authority for Failed Security Practice*, ACMETECH (Sept. 28, 2016), https://www.ssl2048.com/connect/firefox-to-block-chinese-certificate-authority-for-failed-security-practice/ [http://perma.cc/AV7V-JMGD].

121 *See* Patricio Robles, *Can the Blockchain Replace SSL?*, PROGRAMMABLE WEB (Mar. 17, 2015), http://www.programmableweb.com/news/can-blockchain-replace-ssl/analysis/2015/03/17 [http://perma.cc/PL7V-2MF9].

122 MIT researchers have done some of the most cutting-edge work in this field. *See Digital Certificates Project*, MIT, http://certificates.media.mit.edu [https://perma.cc/6FMS-KY3Q] (last visited Nov. 21, 2016).

newly minted, and thus take appropriate precautions. There are several technical and security demands that any such scheme would have to satisfy in the critical infrastructure context and otherwise, but important headway is being made, including by scholars at MIT.[123]

2.4 Application to Critical Infrastructure

"Critical infrastructure" has become an issue of widespread concern, from vulnerable power grids to election systems.[124] Worldwide, many countries are issuing new laws and policies to secure their critical infrastructure even as they struggle to define what should be considered "critical." But the line between critical and non-critical is difficult to draw and is often in the eye of the beholder,[125] though one factor that binds many of these systems together is their mutual reliance on CAs as discussed above.[126]

The task of securing critical infrastructure is daunting, and only seems to be becoming more so. Cyber attacks on U.S. Central Command, Estonia, Georgia, and Iran, among many other incidents, have intensified concerns that hostile foreign governments or non-state actors could preemptively launch cyber attacks on critical infrastructure, including companies that support energy distribution, telecommunications, and financial services.[127] An array of U.S. natural gas pipeline companies and nuclear power plants were reportedly hit in 2013 alone.[128] Because modern societies – as well as large and

---

123 *See id*.

124 *See* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 70 (2010); Scott J. Shackelford at al., *Making Democracy Harder to Hack: Should Elections be Classified as 'Critical Infrastructure?'*, __ MICH. J. OF L. REF. __ (forthcoming 2017).

125 *What is Critical Infrastructure*, DHS, http://www.dhs.gov/what-critical-infrastructure [http://perma.cc/WG5Z-WA5W] (last visited Jan. 16, 2014); *What is the ICS-CERT Mission?*, ICS-CERT, http://ics-cert.us-cert.gov/Frequently-Asked-Questions [http://perma.cc/2THE-PTGT] (last visited Jan. 17, 2014) (The U.S. Cyber Emergency Response Team, which is part of DHS, identifies sixteen critical infrastructure sectors consistent with Homeland Security Presidential Directive 7, including: agriculture, banking and finance, chemical, commercial facilities, dams, defense industrial base, drinking water and water treatment systems, emergency systems, energy, government facilities, information technology, nuclear systems, public health and healthcare, telecommunications, and transportation systems).

126 *See supra* Part 2.3.

127 *See, e.g.*, *Researchers Warn of New Stuxnet Worm*, BBC NEWS (Oct. 19, 2011), http:□□www.bbc.co.uk□news□technology-15367816 [https://perma.cc/MX8A-QRHG] [hereinafter *New Stuxnet*] (reporting on the Duqu exploit and its capacity to attack firms that manufacture industrial control systems).

128 David Goldman, *Hacker Hits on U.S. Power and Nuclear Targets Spiked in 2012*, CNN MONEY (Jan. 9, 2013 1:41 PM EST),

small companies – rely heavily on networked systems and IT to do tasks like payroll, inventory tracking, and research and development, even small-scale cyber operations have the potential to disrupt services and harm public welfare,[129] whereas more substantial exploits could cause paralysis, or worse.[130] According to Professors Christopher Joyner and Catherine Lotrionte, "Western societies have spent years building information infrastructures [in ways] that are interoperable, easy to access and easy to use."[131] Yet the open philosophy of this system is also its Achilles' heel because one infected system can compromise an entire network.

U.S. power systems may become more vulnerable to cyber attacks because of the rise of Internet-connected smart grids called Supervisory Control and Data Acquisition (SCADA) networks.[132] Useful for enhancing efficiency and promoting distributed renewable power, such industrial control systems can increase the cyber threat to critical infrastructure.[133] One senior U.S. military source has said, "[I]f any country were found to be planting logic bombs on the grid, it would provoke the equivalent of the Cuban missile crisis."[134] ."[135] But there is no verifiable public data on how many logic

---

http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks [https://perma.cc/Z5ZN-YGT2] (reporting that "[t]he number of attacks reported to a U.S. Department of Homeland Security cybersecurity response team grew by 52% in 2012" to 198).

129 *See* Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 829–30 (2001); John Reed, *The White House: Cyber Attacks Against Critical Infrastructure Are Way Up*, FP NAT'L SEC. (May 24, 2013), http://killerapps.foreignpolicy.com/posts/2013/05/24/the_white_house_cyber_attacks_against_critical_infrastructure_are_way_up [https://perma.cc/5GTZ-CY5L].

130 *See Cybersecurity Today and Tomorrow: Pay Now or Pay Later*, COMPUTER SCI. & TELECOMM. BD., NAT. RES. COUNCIL 3 (2002).

131 Joyner & Lotrionte, *supra* note 129, at 826.

132 *See, e.g.*, Dana A. Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat*, CONG. RES. SERV.: RL31534 at 1-2 (2003), *available at* https://fas.org/irp/crs/RL31534.pdf [https://perma.cc/FDL9-6JGU]; Elinor Mills, *Just How Vulnerable is the Electrical Grid?*, CNET (Apr. 10, 2009), http://news.cnet.com/8301-1009_3-10216702-83.html [http://perma.cc/XLP2-Z9XQ].

133 *See* Kim Zetter, *Report: Critical Infrastructures Under Constant Cyberattack Globally*, WIRED (Jan. 28, 2010), http:□□www.wired.com□threatlevel□2010□01□csis-report-on-cybersecurity [https://perma.cc/VZ6X-MVHW].

134 COMMITTEE ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 140 n.15 (2010).

135 COMMITTEE ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS, U.S. NATIONAL RESEARCH COUNCIL COMMITTEE ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 140 n.15 (2010) [hereinafter COMMITTEE ON DETERRING

bombs exist, who planted them, and what the legal, economic, or political ramifications might be if they were ever used.[136] From *GhostNet* to Stuxnet and its progeny, cyber weapons have evolved from being considered a supporting component in military operations to systems that are capable of causing actual damage in the real world, including to critical infrastructure.[137] US-CERT has estimated that a significant cyber intrusion occurs every five minutes and that the number of attacks on critical infrastructure jumped some 2,000 percent from 2009 to 2011,[138] while Trend Micro has determined that new pieces of malware are being created at the rate of two per second.[139] In the United States, according to a McAfee report, U.S. "Critical infrastructure owners and operators report that their networks and control systems are under repeated cyberattack, often by high-level adversaries [such as foreign governments]."[140] The consequences of such attacks are potentially devastating. For example, a report by the U.S. Cyber Consequences Unit estimates losses from a major attack on U.S. critical infrastructure at roughly $700 billion.[141] As

---

CYBERATTACKS].

136 Part of the reason for this state of affairs is that the United States has more than 3,200 independent power utilities, unlike Germany, for example, which has four major providers. *See* U.S. DEP'T ENERGY, A PRIMER ON ELECTRIC UTILITIES, DEREGULATION, AND RESTRUCTURING OF U.S. ELECTRICITY MARKETS v. 2.0, at 2.1 (May 2002); CHRISTIAN SCHÜLKE, THE EU'S MAJOR ELECTRICITY AND GAS UTILITIES SINCE MARKET LIBERALIZATION 130 (2010). Some U.S. firms are taking appropriate steps to secure their systems, but differences in resources and expertise makes the uptake of best practices haphazard. *See* Letter from Michael Assante, NERC Vice President and Chief Security Officer, to Industry Stakeholders (Apr. 7, 2009), http://online.wsj.com/public/resources/documents/CIP-002-Identification-Letter-040609.pdf [https://perma.cc/4LMK-TLJ2] (discussing designating critical cyber assets).

137 *See* THOMAS RID, CYBER WAR WILL NOT TAKE PLACE 37–38 (2013); DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER ix–xi (2012); Eric Schmitt & Thom Shanker, *U.S. Debated Cyberwarfare in Attack Plan on Libya*, N.Y. TIMES (Oct. 17, 2011), http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html [https://perma.cc/UZF7-V8MS].

138 *See* Amber Corrin, *Cyber Incident Reports Skyrocket Over Three-Year Period*, FCW (July 2, 2012), http://fcw.com/articles/2012/07/02/ics-cert-report-cyber-attacks-skyrocket.aspx [https://perma.cc/YUR2-K97Y].

139 *See* Dan Dunkel, *Finding the Cure for Cyber Blindness & Missed Opportunities*, SDM (Oct. 17, 2012), http://www.sdmmag.com/articles/88361-finding-the-cure-for-cyber-blindness-missed-opportunities [https://perma.cc/3QDM-JU5W].

140 IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR, MCAFEE CSIS 1 (2009), http://iom.invensys.com/EN/pdfLibrary/McAfee/WP_McAfee_In_The_Crossfire_03-10.pdf [https://perma.cc/7RSK-ZCJZ].

141 *See* JAYSON M. SPADE, INFORMATION AS POWER: CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY 26 (Jeffrey L. Caton ed., 2012) (citing Eugene

such, critical infrastructure cybersecurity has become a central component of U.S. national security, requiring innovative solutions that mitigate the multi-faceted cyber threat from the bottom up, including with regards to CAs and blockchain deployment.

To take one example of the innovation now underway, Guardtime, a cybersecurity firm, is using blockchain technology to secure Britain's power grid, including its nuclear power plants and flood defenses, in collaboration with a startup accelerator, Future Cities Catapult.[142] Guardtime distinguishes its approach to using blockchain in defense of critical infrastructure by leveraging a technology known as Keyless Signature Infrastructure (KSI).[143] This system "relies on the integrity of the hash function to ensure [the] integrity of data" permitting the efficient confirmation of blockchain timing, attribution, and authentication.[144] Deploying this technology in the critical infrastructure context has the potential to avoid compromises such as those taken advantage of in Stuxnet.[145]

In particular, KSI makes it possible to detect "unauthorized changes in software configurations [by] . . . providing a complete chain of the history of the data that is generated and transmitted."[146] Guardtime's KSI blockchain technology is already being deployed to help protect critical infrastructure in Estonia, which is pioneering the use of blockchains to do everything from register marriages to organize health records.[147] It even promises to overcome new technologies that promise to be a boon to both attackers and defenders, such as quantum computing.[148] Most importantly, KSI is distinguished by the fact that it does not rely on CAs and the security issues they raise.[149] Among other features, blockchain technology is mathematically provable, and a relatively simple revocation solution.[150] In practice this can be used to record critical operations, network, and even operating code on the ledger. Thus any attempt by attackers to modify

---

Habiger, *Cyberwarfare and Cyberterrorism: The Need for a New U.S. Strategic Approach*, CYBER SECURE INST., Feb. 1, 2010, at 15–17).

142 *See* Jamie Holmes, *Blockchain For Cybersecurity: Protecting Infrastructure, Data, Telecommunications*, BTC MANAGER (Jan. 7, 2016), https://btcmanager.com/news/tech/blockchain-for-cyber-security-protecting-infrastructure-data-telecommunications/ [https://perma.cc/HG7G-DFT3].

143 *Id*.

144 *See id*. For more on KSI technology, see KSI Blockchain Technology, GUARDTIME, https://guardtime.com/ksi-technology [https://perma.cc/A4UQ-KC6R?type=image].

145 *See* INFOSEC INST., *supra* note 117.

146 *See* GUARDTIME, *supra* note 144.

147 *Id*.

148 *See id*.

149 *See id*.

150 *See id*.

critical data stored on the ledger will be easily found unless attackers are willing to exert extreme computational costs. Similarly, code in critical systems and all approved patching and updating can be stored on the ledger, and the code running in critical systems can be continuously measured against what is recorded in the block-chain. Deviation between the two measurements provides strong evidence for the inclusion of malware on the critical system.

Another firm, BitMesssage, is creating an open-source platform based on "Bitcoin's block-and-transfer system to decentralize and automate encrypted communication."[151] This allows for "transactional mixing," which makes eavesdropping difficult, thereby securing communication lines and allowing defenders to more effectively mitigate cyber risk.[152] The system can also handle a massive amount of Exabyte-scale data while allowing customers to retain privacy through one-way hash functions introduced in Part 1.[153] Similar innovations are underway in the critical infrastructure context of healthcare, particularly with regards to using blockchain technology to safeguard patient data.[154]

MIT researchers have developed another product called Enigma, which was designed "to create a marketplace where users can sell the rights to encrypted data without providing access to the underlying data itself."[155] Although its ultimate impact remains to be seen, the project has the potential guarantee that each packet of data is "masked, random, and . . . secure."[156] If this technology is indeed perfected and rolled out to a mass audience, it would have widespread implications for critical infrastructure security. For example, banks would "be able to store, analyze, and share data" on its customers and investments anonymously. Similarly, healthcare firms would be able to "scan genomic databases for candidates" while guaranteeing "privacy and autonomous control."[157] But as with any new technology, especially one potentially as disruptive as blockchains, the question arises as to whether, and what kind, of regulation may be needed to ensure that the trust engendered by blockchains is not misplaced. A related question centers on whether such regulation is efficient or indeed even possible given the distributed nature of the architecture in

---

151 *Id.*

152 *Id.*

153 *Id.*

154 *See* Megan Molteni, *Moving Patient Data is Messy, but Blockchain is Here to Help*, WIRED (Feb. 1, 2017, 7:00 AM), https://www.wired.com/2017/02/moving-patient-data-messy-blockchain-help/ [https://perma.cc/5EDA-TZW6].

155 *See* GUARDTIME, *supra* note 144.

156 *Id.*

157 *Id.*

question.

3. A ROLE FOR REGULATION AND THE PROMISE OF A POLYCENTRIC BLOCKCHAIN ARCHITECTURE

This final Part builds from the technological primer of Part 1, along with the application section from Part 2, by considering various approaches to blockchain regulation drawing from the work of regulatory modalities pioneered by Professor Lawrence Lessig, among others.[158] Following that, the literature on polycentric institutional analysis is introduced in order to provide a frame for examining multi-level governance options to enshrine cybersecurity best practices in blockchain providers before concluding with implications for managers and policymakers.

3.1 Unpacking the Blockchain Regulatory Landscape

As with any new technology, it is important for regulators to wait until its benefits (and faults) have been uncovered before moving to legislate best practices.[159] If history is any guide, including in the P2P context, "it is likely to be several years before the technology's full potential becomes clear."[160] Unsurprisingly, there currently exists no comprehensive black letter blockchain regulation. The application that has caught the attention of regulators the most up to this point is Bitcoin, but even there most regulators—including the Department of Treasury Financial Crime Enforcement Network—have offered guidance, not formalized rules.[161] Still, a bevy of statutes do touch on blockchain technology (albeit indirectly), and are summarized next to highlight governance gaps and challenges.

Relevant statutes to blockchains include the 1862 Stamp Payments Act,[162] the Securities Act,[163] the Electronic Funds Transfer Act of 1978,[164] and the Bank Secrecy Act, which features the Financial Crimes Enforcement Network to prevent laundering.[165] However, none of these laws are directly

---

158 *See* LAWRENCE LESSIG, CODE: VERSION 2.0 122-125 (2006).

159 *Cf*. Kiviat, *supra* note 9, at 607 ("Blockchain technology is adaptable and policymakers must view it as such. Regulation designed to mitigate the risks of such a powerful technology should be encouraged.").

160 *The Trust Machine*, *supra* note 19.

161 *See* Kiviat, *supra* note 9, at 590.

162 *See* Matthew Kien-Meng Ly, *Coining Bitcoin's "Legal Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies*, 27 HARV. J. L. & TECH. 587, 598-99 (2014).

163 Secs. & Exch. Comm'n v. Shavers, No. 4:13- CV-416, 2014 WL 4652121, at *8 (E.D. Tex. Sept. 18, 2014).

164 15 U.S.C. §§ 1601-1693 (2012).

165 *See* Tsukerman, *supra* note 87, 1157.

applicable to the core focus of this Article being the use of blockchains to enhance cybersecurity of certificate authorities and critical infrastructure. Point agencies for Bitcoin regulation have included the FBI, which (temporarily) shut down Silk Road, a site for trading illicit property using Bitcoins.[166] The IRS has also gotten involved in both Bitcoin and blockchain regulation, notably in March 2014 when it issued a notice stating that the agency would treat Bitcoins as property, not a currency, in a move creating an array of complex income tax liabilities.[167] Similarly, the Commodity Futures Trading Commission (CFTC), which regulates commodities futures, arguably has the authority to regulate Bitcoin price manipulation, which, if accurate, could open up a slew of regulatory avenues for regulators to explore.[168] And even the Consumer Financial Protection Bureau's (CFPB) mission to "make markets for consumer financial products and services work for Americans"[169] implicates Bitcoin and blockchain technology; indeed, the CFPB has already issued a "consumer advisory statement" in Bitcoins in August 2014 warning the public about the risks.[170]

Some states, such as New York, have gone further. New York in particular has required the placement of certain cybersecurity safeguards in blockchain applications in the name of consumer protection under the BitLicense scheme, increasing the cost of compliance to market entrants and prompting some firms at least to leave the New York market.[171] Californian officials, particularly within the Department of Business Oversight, have also decided that state law applies to crypto-currencies like Bitcoin.[172]

More innovation is happening globally with a variety of nations moving to regulate blockchain applications including Bitcoin, as seen in the European Union's 2015 decision to recognize Bitcoin as a currency referenced in Part 1.[173] Yet

---

166 *Id*. at 1158.

167 INTERNAL REVENUE SERVICE, IRS VIRTUAL CURRENCY GUIDANCE: VIRTUAL CURRENCY IS TREATED AS PROPERTY FOR U.S. FEDERAL TAX PURPOSES; GENERAL RULES FOR PROPERTY TRANSACTIONS APPLY (Mar. 25, 2014), http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance [https://perma.cc/S9AD-42WN].

168 Tsukerman, *supra* note 87, at 1161.

169 *About Us*, CONSUMER FINANCIAL PROTECTION BUREAU, http://www.consumerfinance.gov/the-bureau/ [https://perma.cc/YLM8-XS47].

170 Tsukerman, *supra* note 87, at 1161.

171 *Id*. at 1163.

172 *See* Michael B. Marois & Carter Dougherty, *California Says State Law Grants Right to Oversee Bitcoin*, BLOOMBERG (Dec. 4, 2014 4:28 PM), http://www.bloomberg.com/news/2014-12-04/california-says-state-law-grants-right-to-oversee-Bitcoin.html [https://perma.cc/97Q3-9Z5L].

173 *The Trust Machine*, *supra* note 19.

such multi-jurisdictional regulation also raise enforcement challenges given that a policy imposed by one stakeholder—such as New York—may conflict with another, potentially leading to a forked chain as discussed in Part 1.2.3. In such an instance, some jurisdictions could elect to ban the technology, which in the U.S. context could lead to First Amendment issues given that code has already been defined as speech.[174] Another potential scenario would be judges issuing rulings that, perhaps inadvertently, cause such hard forks, such as by ordering that one transaction be approved over another conflicting one.[175] But black letter law is just the beginning of blockchain regulation, which, after all, does quite a bit to regulate itself. After all, it is the inherent self-correcting "security of the system" that "makes the blockchain revolutionary."[176]

Taking a broader view, blockchain regulation is happening at various levels and through various modalities beyond black letter law, including, to use Professor Lawrence Lessig's nomenclature, norms, markets, and code,[177] as well as self-regulation, and multilateral collaboration, all of which can contribute to enhancing critical infrastructure cybersecurity through blockchains. For example, best practices developed by blockchain technology providers—such as Ethereum, discussed in Part 1.3—inform the behavior of peer competitors, and (depending on uptake) can lead to industry norms and codes of conduct, which may in turn eventually be codified, as has happened in the power grid context. Each of these regulatory approaches has unique benefits and drawbacks, but together they contribute to a governance regime that is multi-level, multi-purpose, multi-type, and multi-sectoral in scope and that could complement the top-down critical infrastructure governance models favored by certain nations.[178] Next, we dig

---

174 *See, e.g.*, CHRISTOPHER WOLF, THE DIGITAL MILLENNIUM COPYRIGHT ACT: TEXT, HISTORY, AND CASELAW 1053-55 (2003); Scott J. Shackelford et al., *iGovernance: The Future of Multi-Stakeholder Internet Governance in the Wake of the Apple Encryption Saga*, __ UNIV. OF N. CAROLINA J. OF INT'L L. __ (forthcoming 2017) (manuscript at 17 n. 77); Adam Satariano, *Apple-FBI Fight Asks: Is Code Protected as Free Speech?*, BLOOMBERG TECH. (Feb. 23, 2016 7:55 PM), https://www.bloomberg.com/news/articles/2016-02-24/apple-fbi-fight-asks-is-code-protected-as-free-speech [https://perma.cc/7KS2-D3T8].

175 *See, e.g.*, Primavera de Filippi, *A $50M Hack Tests the Values of Communities Run by Code*, MOTHERBOARD (July 11, 2016), http://motherboard.vice.com/read/thedao [https://perma.cc/PF86-8QYH].

176 Tsukerman, *supra* note 87, at 1136 (noting "Security in the Bitcoin protocol is ensured through 'cryptographic proof,' allowing the parties to deal directly with each other, rather than through a third party.").

177 *See* LESSIG, *supra* note 158, at 124-125.

178 For more on this topic, see Scott J. Shackelford & Amanda N. Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 119 (2014).

into the potential of a distributed governance model to match the distributed technology at the heart of Bitcoin.

3.2 A Primer on Polycentric Governance: From Polanyi to the Present

It may be easiest to understand polycentric governance in juxtaposition to the alternative—monocentrism, which is a political system where the authority to enforce rules is "vested in a single decision structure that has an ultimate monopoly over the legitimate exercise of coercive capabilities."[179] At its core—building from important notions of legitimacy, power, and multiple decision centers—polycentric governance is concerned with the rule of law. In this manner, the U.S. constitution has been described as an "experiment in polycentricity" with federalism being one way to operationalize the concept.[180] What is it that makes polycentric systems so special? In short, the capacity for spontaneous self-correction.[181] In the words of Professor Elinor Ostrom, "a political system that has multiple centers of power at differing scales provides more opportunity for citizens and their officials to innovate and to intervene so as to correct maldistributions of authority and outcomes. Thus, polycentric systems are more likely than monocentric systems to provide incentives leading to self-organized, self-corrective institutional change."[182]

A key element of polycentricity is this spontaneity, which to Professor Vincent Ostrom meant that "patterns of organization within a polycentric system will be self-generating or self-organizing" in the sense that "individuals acting at all levels will have the incentives to create or institute appropriate patterns of ordered relationships."[183] What factors are most important to engender such spontaneous self-correction? Free entry, and the incentivized enforcement of rules, which are in turn continually revised.[184] In other words, anyone should be able to play the game, and even collaborate to change the rules through orderly means. This requires that procedural (e.g., rules for changing rules) and cognitive (understanding of relationships) preconditions be met.[185] As such, "[i]nstitutional design, the application of our understanding of rules and consequences and the conditions that determine their

---

179 Paul D. Aligica & Vlad Tarko, *Polycentricity: From Polanyi to Ostrom, and Beyond*, 25 GOVERNANCE 237, 245 (2012).

180 *Id.*

181 *Id.* at 246.

182 *Id.*

183 *Id.*

184 *Id.*

185 *Id.* at 247.

interplay, is part and parcel of spontaneous order and not inimical to it."[186]

The "basic idea" of polycentric governance, according to Professor Michael McGinnis, is that a group facing a collective action problem "should be able to address" it in "whatever way [the members of the group] best see fit."[187] This could include using existing governance structures or crafting new systems.[188] Polycentric governance regimes that are multi-level, multi-purpose, multi-type, and multi-sectoral in scope[189] could complement existing multi-stakeholder models of Internet governance, which has enjoyed a more organic development trajectory.[190] Yet this trend is a double-edged sword with many nations seeking to assert greater control online, challenging the notion of cyberspace as a commons and further fracturing governance at a time of increasing cyber insecurity.[191]

Professor Michael Polanyi was an early pioneer in the field of polycentric governance, recognizing that polycentric structures are vital for scientific discovery given that the inherent "freedom is utilized to search for an abstract end goal (objective truth)."[192] In such a polycentric system, ideas of equity and justice, Polyani argued, may only be crystallized by a gradual process of trial and error experimentation.[193] Professor Lon Fuller agreed with Polyani's assessment with regards to polycentrism, arguing that many legal decisions are in fact polycentric in that they involve multiple "decision centers and the network of cause and effect relationships is not

---

186 *Id*.

187 Michael D. McGinnis, *Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care* 1, (Ind. Univ. Vincent and Elinor Ostrom Workshop in Political Theory and Policy Analysis, Working Paper W11-3, 2011), http://php.indiana.edu/~mcginnis/Beijing_core.pdf [https://perma.cc/52SR-Q3AX].

188 *Id*. at 1-2.

189 Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39 POL'Y STUD. J. 163, 171 (2011) (defining "polycentricity" as "a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes.").

190 *See* Chapter 1 in SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

191 *See* Paul Tassi, *The Philippines Passes a Cybercrime Prevention Act that Makes SOPA Look Reasonable*, FORBES (Oct. 2, 2012, 8:04 AM), http://www.forbes.com/sites/insertcoin/2012/10/02/the-philippines-passes-the-cybercrime-prevention-act-that-makes-sopa-look-reasonable/.

192 Aligica & Tarko, *supra* note 179, at 238.

193 *Id*. at 239.

understood very well."[194] Such a conceptualization of the justice system highlights, among other issues, the prevalence of unintended consequences that can frustrate justice seekers,[195] unintended consequences that can quickly spread in the context of a distributed technology like blockchains.

The Ostroms' work on polycentric governance, begun in the 1960s, was initially centered on questions of metropolitan governance, but subsequently evolved in two directions—social theory, and empirical investigations of governance structures. They challenged the majority view at the time that the "problem of metropolitan government" was that "the multiplicity of political units" made effective governance difficult, if not impossible.[196] To this notion, the Ostroms contended that "the optimum scale of production is not the same for all urban public goods and services."[197]

The Ostroms argued that coordination in complex systems is in fact possible through interorganizational arrangements that "would manifest market-like characteristics and display both efficiency-inducing and error-correcting behavior."[198] In other words, by taking a political economy approach, the Ostroms were able to show that "competition among public agencies is not necessarily inefficient."[199] Yet the great leap in governance research was the Ostroms' contention to test their presumption, "to undertake critical tests where divergent theories imply contradictory conclusions."[200] This was the birth of empirical, polycentric governance research, the ramifications of which continue to resonate around the world in a wide array of contexts to this day.

Among the first propositions studied was the claim that "the size of the governmental unit affects the output and efficiency of service provision," in other words, that governance size matters.[201] The Ostroms undertook this work first in Indianapolis—comparing the performance of smaller police departments against the larger Indianapolis City Police Department—before moving on to examine other municipalities, including Chicago, St. Louis, Grand Rapids, and

---

194 *Id*. at 240.

195 *Id*.

196 *Id*. at 241.

197 *Id*.

198 *Id*. at 242 (quoting Vincent Ostrom & Elinor Ostrom, *A Behavioral Approach to the Study of Intergovernmental Relations*, 359 ANNALS OF THE AMERICAN ACADEMY OF POLITICAL AND SOCIAL SCIENCE 135-137 (1965)).

199 *Id*.

200 *Id*. (quoting Vincent Ostrom & Elinor Ostrom, *A Behavioral Approach to the Study of Intergovernmental Relations*, 359 ANNALS OF THE AMERICAN ACADEMY OF POLITICAL AND SOCIAL SCIENCE 135-137 (1965)).

201 *Id*.

Nashville.[202] In short, they found that: "The presumption that economies of scale were prevalent was wrong; the presumption that you needed a single police department was wrong; and the presumption that individual departments wouldn't be smart enough to work out ways of coordinating was wrong."[203] On the whole, "polycentric arrangements with small, medium, and large departmental systems generally outperformed cities that had only one or two large departments"[204] What do police departments have to do with blockchains? These findings were an early indication of the power of distributed governance to build trust in complex systems. But the success of these systems is not automatic.

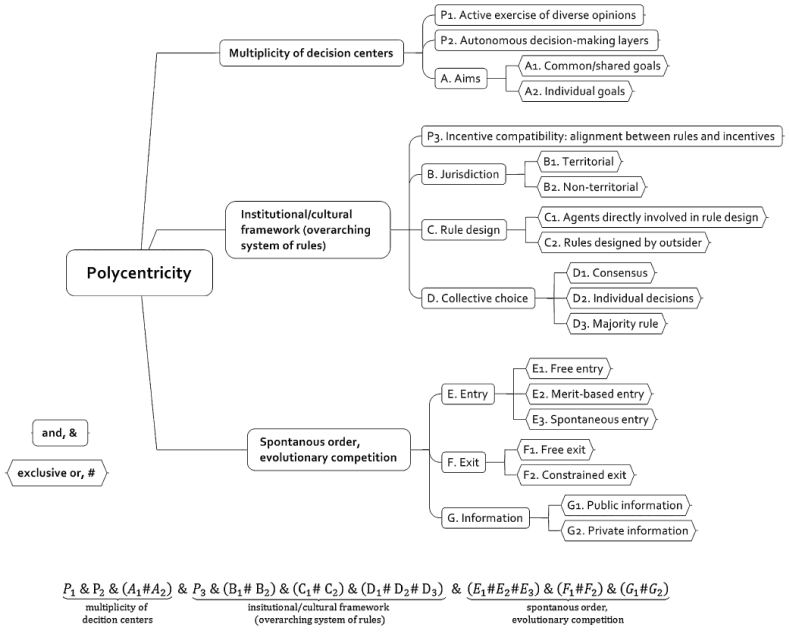
In summary, the three main features of polycentric governance may be described in terms of the: (1) "multiplicity of decision centers[, which] is analyzed in terms of those centers' ability to implement their different methods into practice . . . the presence of autonomous decision-making layers, and . . . the existence of a set of common/shared goals;"[205] (2) "institutional and cultural framework that provides the overarching system of rules defining the polycentric system . . . in terms of whether the jurisdiction of decision centers is territory based or superimposing, . . . whether the decision centers are involved in drafting the overarching rules, . . . whether the rules are seen as useful by the decision centers (regardless of whether or not they are involved in their drafting—that is, the alignment between rules and incentives) and in terms of the nature of the collective choice aggregating mechanism (market, consensus, or majority rule);"[206] and (3) "spontaneous order generated by evolutionary competition between the different decision centers' ideas, methods, and ways of doing things, [which] is analyzed in terms of whether there exists free exit, . . . the relevant information for decision making is public . . . and finally, in terms of the nature of entry in the polycentric system—free, meritocratic, or spontaneous."[207] To put it another way, the preconditions for polycentricity include the "active exercise" of differing preferences that are implemented in the real world,[208] as well as "incentives compatibility," meaning that the rules are considered "useful by the agents subjected to them."[209] Equally important is "autonomous decision-making" featuring

---

202 *Id.* at 243.
203 *Id.*
204 *Id.*
205 *Id.* at 254.
206 *Id.*
207 *Id.*
208 *Id.* at 255.
209 *Id.* at 256.

"overlapping decision centers."[210] Together, this literature, although based on a relatively small number of cases, enjoys a potentially wide application,[211] a topic illustrated in Figure 8, which shows some 288 differing polycentric systems from the indicators identified.[212]

Figure 8: Logical Structure of Polycentricity[213]



What does all this mean in terms of predicting when polycentric systems may fail? In particular, the model suggests that this may indeed happen when: (1) The "[m]ultiplicity of decision centers breakdown due to the system becoming hierarchical or when the desired goal is achieved";[214] (2) The "[o]verarching system of rules breakdown" due to, for example, the rules no longer being considered useful confused;[215] and (3) The central spontaneity criterion breaks down due to, for example, barriers to entry.[216] As applied to blockchains, then, problems may arise due to either multi-jurisdictional strife or the undue centralization of regulation, along with related problems of barriers to entry due possibly to inadequate incentives to perpetuate mining. If these conditions may be

210 *Id.*
211 *Id.*
212 *Id.* at 257.
213 *Id.*
214 *Id.* at 258.
215 *Id.*
216 *Id.*

overcome, then it may be possible to "provide a way of discovering how to improve the functioning of different configurations and complex social systems by means of drawing analogies between them. Different complex systems have weak and strong points. The challenge is how to bring the strong points from one area into another in order to counter the weak points."[217] One of the ways that polycentric governance is operationalized is through Ostrom design principles, the topic we turn to next.

3.3 Building Trust through Blockchains – Applicability of the Ostrom Design Principles

In her groundbreaking 1990 book *Governing the Commons*, Professor Ostrom laid out an informative framework of eight design principles for the effective management of CPRs.[218] These principles were distilled from the common traits that Ostrom discovered through her meta-analysis of successful common property regimes.[219] The design principles, in turn, are helpful in making predictions about the governance of CPRs under various scenarios, and include the importance of: (1) "clearly defined boundaries for the user pool . . . and the resource domain";[220] (2) "proportional equivalence between benefits and costs";[221] (3) "collective choice arrangements" ensuring "that the resource users participate in setting . . . rules";[222] (4) "monitoring . . . by the appropriators or by their agents";[223] (5) "graduated sanctions" for rule violators;[224] (6) "conflict-resolution mechanisms [that] are readily available, low cost, and legitimate";[225] (7) "minimal recognition of rights to organize";[226] and (8) "governance activities [being] . . . organized in multiple layers of nested enterprises."[227] Not all of Professor Ostrom's design principles are applicable to

---

217 *Id*. at 260.

218 *See* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 90 (James E. Alt & Douglass C. North eds., 1990).

219 *See* Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems* 408, 422 (Nobel Prize Lecture, 2009), http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2009/ostrom_lecture.pdf.

220 SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 32 (1998).

221 *See* OSTROM, *supra* note 219.

222 BUCK, *supra* note 220.

223 *Id*.

224 *Id*.

225 *Id*.

226 Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES INVOLVING A DIVERSITY OF ORGANIZATIONS 105, 118 tbl. 5.3. (Eric Brousseau et al. eds., 2012).

227 *Id*.

blockchains. However, some do have salience, and are addressed in turn to inform a discussion of appropriate policy responses to global collective action problems.

3.3.1 Defined Boundaries

According to Professor Ostrom, "The boundary rules relate to who can enter, harvest, manage, and potentially exclude others' impacts. Participants then have more assurance about trustworthiness and cooperation of the others involved."[228] This design criterion could be applied to blockchain developers in different ways depending on whether one is considering a fully public, transparent distributed ledger, or a private blockchain internal to a particular firm or industry. If the latter, then the members of the group would need to be vetted since, once inside, they could have unfettered access to everything recorded on the register.

3.3.2 Proportionality

This design principle underscores the need for equity in a system so that some of the "users [do not] get all the benefits and pay few of the costs . . . ."[229] This principle evokes debate over the core question about how best equity should be encouraged in blockchain platforms. In some ways, blockchains could be seen as encouraging greater equity by enhancing transparency, user participation, and rewarding contributions with fees. This may be especially true in redesigned platforms that do not require as much computing power as the Bitcoin blockchain, though this may further increase the need for trusted systems.[230] More generally, the equity criterion speaks to the importance of ensuring that the benefits of blockchains are widely distributed beyond sophisticated multinational firms, a process that could eventually require training programs as new products and even governmental services are rolled out.

3.3.3 Collective-Choice Arrangements and Minimal Recognition of Rights

Professor Ostrom's third design principle states "that most of the individuals affected by a resource regime are authorized to participate in making and modifying the rules

---

228 *Id.* at 119.
229 *Id.* at 120.
230 *The Trust Machine*, *supra* note 19.

related to boundaries, assessment of costs . . . , etc."[231] This principle implies the importance of engaged and proactive rulemaking by technical communities, the private sector, and the international community.[232] Such a multi-stakeholder approach is part and parcel of how the Bitcoin blockchain has been developed, and is continuously fixed as new bugs are found and exploits created as was discussed in Part 1.2. It will be imperative to copy the success of this program, while ensuring that even broader, non-technical sections of the citizenry are involved with discussions of blockchain governance best practices to avoid situations in which the better off make the rules. This happens in the Bitcoin context, for example, when those with all the Bitcoins on the system make the rules on hard-forks, as was discussed in Part 1.2.3.

3.3.4 Monitoring

According to Professor Elinor Ostrom, trust can typically only do so much to mitigate rule-breaking behavior.[233] Eventually, some level of monitoring becomes important. In self-organized communities, typically monitors are chosen among the members to ensure "the conformance of others to local rules."[234] However, in the cyber context verification becomes difficult, to say the least. But again, this is something that especially public blockchain technologies do exceedingly well. Instead of relying on external authorities such as CAs or a small number of entities to patrol errant behavior, given that the public ledger is transparent and distributed for public blockchains, anyone can act as a monitor, a form of private attorney general of the kind used to enforce certain environmental laws.[235]

3.3.5 Graduated Sanctions and Dispute Resolution

Other insights from Professor Ostrom's principles such as the need for graduated sanctions for rule violators and effective dispute resolution speak to the importance of addressing legal ambiguities and establishing norms of behavior. The former point underscores the significance of not

---

231 Ostrom, *supra* note 226, at 120.

232 *See* George J. Siedel & Helena Haapio, *Law as a Source of Strategic Advantage: Using Proactive Law for Competitive Advantage*, 47 AM. BUS. L.J. 641, 656–57 (2010) (discussing the origins of the proactive law movement, which may be considered "a future-oriented approach to law placing an emphasis on legal knowledge to be applied before things go wrong.").

233 Ostrom, *supra* note 226, at 120.

234 *Id* at 121.

235 *See, e.g.*, Henry Cohen, *Awards of Attorneys' Fees by Federal Courts and Federal Agencies*, *in* LAW AND ECONOMIC ENFORCEMENT ISSUES 253, 257 (Gerald M. Kessler, ed., 2008).

"[l]etting an infraction pass unnoticed,"[236] meaning that the cost of flouting cyber norms need to be recognized through some combination of market reaction and governmental action. This would be especially important if blockchains are widely deployed in the critical infrastructure context, given how vital these services are to the continued functioning of the global economy. Yet anonymity of blockchain applications like Bitcoin could exacerbate these challenges.

3.3.6 Nested Enterprises

As stated by Professor Ostrom, "[w]hen common-pool resources that are being managed by a group are part of a larger set of resource systems, an eighth design principle is usually present in robust systems. The nested enterprise principle states that governance activities are organized in multiple layers of related governance regimes."[237] Blockchains fit within this definition of nested enterprises in that they feature multiple layers, represented by hashes, that have the added bonus of a temporal feature, allowing anyone to track transactions, and for that matter how norms themselves have evolved over time. This technology, consequently, provides an opportunity for the study of temporal norm development within the cybersecurity context across numerous platforms in the critical infrastructure context and beyond. Further study is needed in this regard.

3.3.7 Summary

As helpful as Ostrom's design principles are to analyzing the factors necessary to create a functioning system of polycentric governance to conceptualize governance and build trust in distributed systems like blockchains, they are far from perfect, as Professor Ostrom would be the first to admit.[238] There are, for example, gridlock concerns along with moral and political problems in play, including an application of Garrett Hardin's "lifeboat ethics."[239] Though Professor Ostrom's important work on the principles, along with the Institutional Analysis and Design (IAD) Framework, often gets much of the

---

236 Ostrom, *supra* note 226, at 121.

237 *Id.* at 122.

238 *See* Elinor Ostrom et al., *Revisiting the Commons: Local Lessons, Global Challenges*, 284 SCI. 278, 282 (1999) (noting that some of her work in the global commons context to "provide starting points for addressing future challenges.").

239 Garrett Hardin, *Lifeboat Ethics: The Case Against Helping the Poor*, PSYCHOL. TODAY, Sept. 1974, at 800 (examining, from an ethical viewpoint, when swimmers surrounding a lifeboat should be taken aboard).

attention in public policy circles given its emphasis on self-understanding beyond classical rational choice rather than black letter law,[240] her work on the Social-Ecological-Systems (SES) Framework beginning in approximately 2007 offers an even more "comprehensive approach to the study of closely-coupled systems" drawing from both social and ecological factors.[241] Still, though, running throughout her work is an empirical demonstration that "public services can be most efficiently provided under a system of multiple and overlapping jurisdictions . . . ."[242] New blockchains startups should be aware of the key findings of both bodies of literature summarized next. After all,"[p]olycentricity can be utilized as a conceptual framework for drawing inspiration not only from the market but also from . . . other complex system incorporating the simultaneous functioning of multiple centers of governance and decision making with different interests, perspectives, and values."[243]

3.4 Implications for Managers and Policymakers

The promise of blockchain technology has expansive applications across a range of cybersecurity sectors, including in the CA and critical infrastructure context, as has been explored throughout this Article. The implications on organizational decision-making are manifold, ranging from the way that ledgers are created and transactions recorded, to new product lines designed to build trust in insecure systems. Managing the risks and rewards presented by such a disruptive pivot point presents numerous opportunities and challenges for managers and policymakers alike, some of which are discussed here beginning with the private sector before moving on to extending our analysis to related arenas such as the burgeoning Internet of Things.

The widespread use of blockchains will inevitably mean business disruption. After all, all businesses—and indeed entire industries that are now in the "trust business"—will need to adapt, or otherwise remake themselves.[244] For example, blockchains could be further tailored, such as by rolling out new rules such as transactions only being cleared if they are endorsed by multiple parties.[245] Institutional memory would be

---

240 Michael D. McGinnis, *Elinor Ostrom: Politics as Problem-Solving in Polycentric Settings*, *in* ELINOR OSTROM AND THE BLOOMINGTON SCHOOL OF POLITICAL ECONOMY 281, 285, 292 (Daniel H. Cole & Michael D. McGinnis eds., 2014).

241 *Id*.

242 *Id*. at 286.

243 *Id*. at 260.

244 *The Trust Machine*, *supra* note 19

245 *Id*.

a organizations for firms of all sizes deploying blockchains. As with Napster and P2P file sharing, this type of evolution takes time, but such experimentation in the name of building trust is at the heart of the polycentric governance literature, and is squarely in line with the needs of critical infrastructure providers to secure their systems. The same goes for an array of governmental services, which could, if the myriad benefits of blockchain technology are in fact realized, handle most major life events—from a birth certificate, to a marriage license, property deed, and even a death certificate—with minimal human interference.[246] However, there are also limitations to this technology, as are summarized below.

At a higher level, the history of finance would be an open book, potentially being a boon to sustainability and the Corporate Social Responsibility (CSR) movement. Indeed, sustainability may well be a useful paradigm to explore for lessons that could be imported to enhance the prospects for successful blockchain governance. There is a growing body of work investigating, for example, intersections between the green movement, cybersecurity, and Internet governance, including the applicability of international environmental law principles to such collective action problems as information pollution.[247] Similarly, an underappreciated overlap occurs in the blockchain context by considering the literature on software ecology and ecosystems with blockchain governance best practices. In this vein, Bitcoin itself could be considered a common pool resource in that the public is contributing the resource in terms of time and computing power to create and transact Bitcoins, with governance of the system being distributed and shared globally.[248] Such common pool resources are exhaustible, and are managed through a property regime in which enforcing the exclusion of a "defined user pool" can be difficult.[249] Common examples of common pool resources

---

246 *Id*.

247 *See, e.g.*, Scott J. Shackelford, Timothy L. Fort, & Danuvasin Charoen, *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 U. ILL. L. REV. 1995; Scott J. Shackelford, *On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems*, 18 VAND. J. ENT. & TECH. L. 653(2016).

248 *See* SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 2-5 (1998) (explaining that common pool resources implicate property rights and are defined as "subtractable resources managed under a property regime in which a legally defined user pool cannot be efficiently excluded from the resource domain").

249 *Id*. at 5; *see also* Joseph S. Nye Jr., *Cyber Power*, HARV. BELFER CTR. 15 (2010), http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf [https://perma.cc/D8VZ-EXB8] (making the case that cyberspace may be considered a type of common pool resource, and as such 'self-organization is

include some fisheries, pastures, and forests. What do fisheries have to do with cybersecurity? The difficulties of enforcement and overuse bind these areas together, while similar issues of scale (such as the size and number of Bitcoin transactions) echo in other commons arenas. However, Bitcoin and its underlying blockchain technology may similarly have insights that could be applied toward enhancing the governance of other classic common pool resources. Communities could learn from the power of blockchain technology to register users (or even job candidates[250]) and keep track of transactions, allowing, for example, the ability to recognize and trace complex common property relationships without the need for state intervention.[251]

A further area that deserves deeper exploration, especially in the legal literature, is the application of blockchain technology to Internet of Things applications. There is a great deal of buzz surrounding the Internet of Things (IoT), which is the notion, simply put, that nearly everything not currently connected to the Internet, from gym shorts to streetlights soon will be.[252] The rise of "smart products" such as Internet-enabled refrigerators and self-driving cars holds the promise to revolutionize business and society. Applications are seemingly endless, and embrace an array of consumer products, including toasters.[253] As stated by Dan and Alex Tapscott, "[h]ow about these billions of connected smart things that will be sensing, responding, sharing data, generating and trading their own electricity, protecting our environment, managing our homes and our health? And this Internet of Everything will need a *Ledger of Everything*."[254] Regardless of

---

possible under certain conditions.'").

250 *See* Kinni, *supra* note 93 ("Companies like ConsenSys are developing identity systems where job prospects or prospective contractors will program their own personal avatars to disclose pertinent information to employers. They can't be hacked like a centralized database can. Users are motivated to contribute information to their own avatars because they own and control them, their privacy is completely configurable, and they can monetize their own data. This is very different from, say, LinkedIn, a central database owned, monetized, and yet not entirely secured by a powerful corporation.").

251 For more on this topic, see Scott J. Shackelford, *Neither Magic Bullet Nor Lost Cause: Land Titling and the Wealth of Nations*, 21 NYU ENVTL. L. J. 272 (2014).

252 *See* Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341, 348 (2015); Daniel Burrus, *The Internet of Things is Far Bigger than Anyone Realizes*, WIRED (Nov. 2014), http://www.wired.com/2014/11/the-internet-of-things-bigger/ [https://perma.cc/V3UZ-JBD8].

253 *See* Richard Baguley & Colin McDonald, *Appliance Science: The Internet of Toasters (and Other Things)*, CNET (Mar. 2, 2015), https://www.cnet.com/news/appliance-science-the-internet-of-toasters-and-other-things/ [https://perma.cc/9CV9-6B55].

254 Tapscott & Tapscott, *supra* note 1.

whether this is, in fact, necessary, the potential for blockchains to aid in securing this range of systems requires further unpacking and research surrounding interlinked governance best practices.

The downsides of blockchain technology also need to be carefully considered, least of which is the fact that—in a public blockchain—everything is public, forever.[255] This recalls debates over the "right to be forgotten," raising the specter of regulation, which could, in turn, be ineffective if its domestic share of the global blockchain was less than fifty percent of available computing power. Other outstanding issues also deserve consideration from managers and policymakers alike, including longevity and governance. As such, it should be clear that, despite their power, blockchains are not a panacea. For example, despite ongoing concerns about the security of the U.S. election system, including pervasive vulnerabilities on voting machines run by thousands of jurisdictions across the country,[256] the utility of blockchain technology to make democracy harder to hack is limited.A national election with significant national security implications would be a rapid target for criminal organizations and nation states. If any one group—or some combination of these groups—were to achieve more than fifty percent of the computing power on the blockchain, they could tamper with the results.[257] Further, introducing millions of voters to blockchain technology—and creating a system robust enough to scale upward—would raise significant technical challenges.[258]

Still, if privacy concerns and other considerations are overcome, the benefits of blockchain technology are indeed immense. Indeed, the goals of blockchain proponents are "laudable," including "speed, lower cost, security, fewer errors, and the elimination of central points of attack and failure."[259] Consequently, although such a future will doubtless intimidate or otherwise cause some consternation across various stakeholders, given declining trust in both public and private-

---

255 Kinni, *supra* note 93.

256 *See, e.g.*, Scott J. Shackelford, *Opinion: How to Make Democracy Harder to Hack*, CHRISTIAN SCI. MONITOR (July 29, 2016), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0729/Opinion-How-to-make-democracy-harder-to-hack [http://perma.cc/4AX3-DK2J].

257 *See supra* note 95 and accompanying text (discussing the possibility of hacking a blockchain by accumulating more than fifty percent of the computer power in the distributed network).

258 For more on this topic, see Sunoo Park & Ronald L. Rivest, Towards Secure Quadratic Voting (2016) (unpublished manuscript), http://people.csail.mit.edu/sunoo/p/17/qv.pdf [http://perma.cc/C9EK-K7ZX].

259 Tapscott & Tapscott, *supra* note 8.

sector institutions,[260] any effort to build transparency, reduce costs, and improve security will likely be welcomed by the majority.

CONCLUSION

To many, the notion of blockchains and distributed ledgers is the stuff of cocktail-party conversation stoppers. Other similar innovations, from double-entry bookkeeping or joint-stock companies, can also solicit a shrug—though it should be noted that some scholars have argued that these inventions "enabled the rise of capitalism and the nation-state."[261] But, as with these earlier practices, blockchains have the potential to, simply put, "transform how people and businesses co-operate."[262] Such an outcome is by no means pre-determined with an array of technological, economic, political, and governance issues to be overcome;[263] still, the promise of this technology, especially in the context of enhancing cybersecurity in CAs and related critical infrastructure systems, deserves our sustained attention.[264] In other words, a sustainable blockchain edifice will not be built overnight, it will take ongoing attention by numerous stakeholders—including policymakers—over a period of years, perhaps decades. But by starting now, block by block, we can build trust in an age that has to date been defined by increasing cyber insecurity.

---

260 *See* Jim Norman, *Americans' Confidence in Institutions Stays Low*, GALLUP (June 13, 2016), http://www.gallup.com/poll/192581/americans-confidence-institutions-stays-low.aspx [http://perma.cc/ZN6B-FK6C].

261 Tapscott & Tapscott, *supra* note 8.

262 *The Trust Machine*, *supra* note 19.

263 *See, e.g.*, Ben Dickson, *Before you Invest in a Blockchain Startup, Read This*, VENTURE BEAT (Dec. 10, 2016), http://venturebeat.com/2016/12/10/before-you-invest-in-a-blockchain-startup-read-this [http://perma.cc/2YER-9DTQ].

264 Other related arenas in which blockchain technology could enhance distributed trust include the supply chain for digital goods, hashes for software distributions and patches, and potentially even a distributed ledger to promote confidence in "real" news. *See, e.g.*, Michael Casey & Oliver Luckett, *Here's How to Fix Facebook's Fake News*, DAILY BEAST (Nov. 19, 2016), http://www.thedailybeast.com/articles/2016/11/19/here-s-how-to-fix-facebook-s-fake-news.html [http://perma.cc/FN3J-2HLF].

APPENDIX A: A SHORT INTERLUDE INTO CRYPTOGRAPHY

This Appendix briefly lays out some of the relevant cryptographic principles underlying blockchain technology, beginning with hash functions before moving on to digital signatures and Bitcoin transactions.

Hash Functions

A function is simply a map of objects in one set, called the domain, to another set of objects, called the range. For example, a primary school function $f(x)=x+4$ is another way of mapping numbers to other numbers. We denote this by writing $f:N\rightarrow N$, to show that the function maps integers to integers, or $f:R\rightarrow R$ to compare real numbers to real numbers. A function that maps a large, possibly infinite, set of objects to a smaller set of objects is called a hash function. For example, a function $g(x)=\lfloor x/2 \rfloor$, divides x by 2, and rounds down to the nearest integer. When we constrain the domain and range of g as follows, $g:\{1,2, \ldots ,12\}\rightarrow\{1,2 \ldots ,6\}$, this becomes a hash function that maps the integers between 1 and 12, the range, to integers between 1 and 6, the domain. Since the domain is larger than a range it is a hash function. For any elements $x \neq x'$ for which $g(x)=g(x')$, we say that x and x' *collide*, or that there is a *collision.* Note that by the Pigeon Hole Principle,[265] all hash functions have collisions.

Cryptographic Hash Functions

Cryptographers are interested in hash functions with specific properties, which are too technical to present formally here, so instead we will focus on the high-level intuition. Two properties of interest for the immediate purposes are *pseudo-randomness* and *collision resistance,* which are two properties that together allow cryptographers to treat the hash function as a *Random-Oracle.* To aid in the explanation, it helps to have a specific hash function in mind. The one used in Bitcoin is the National Institute of Standards and Technology (NIST) cryptographically approved hash function SHA256, where $SHA256:\{0,1\}^*\rightarrow \{0,1\}$.[266] That is, it maps any finite binary

---

265 The Pigeon Hole Principle states that if you have a set of n objects, mapped to a set of m containers n>m, then there are at least two objects mapped to the same container. The concept is helpful when dealing with finite sets.

266 *See* SECURE HASH STANDARD, NIST (Aug. 2015), http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf [http://perma.cc/K7NY-6AJ3].

string (denoted $\{0,1\}^*$) to a binary string of length 256 bits (denoted $\{0,1\}^{256}$). Further, for the discussion that follows, the size of the range is 2^{256}, which is truly an astronomically large number: there are estimated to be "only" approximately 2^{267} atoms in the observable universe.[267]

A hash-function is pseudo-random when given a random input x of a fixed size (say 256 bits) that is unknown to an efficient adversary, and the output is indistinguishable from a truly random outcome to the same adversary. For example, the output of the SHA256(x)||SHA562(x||1)||SHA256(x||11)||SHA256(x||111)|| . . . hash appears random to an *efficient* adversary that does not know x, but which has full knowledge of the hash function SHA256. Here, an efficient adversary can be considered someone that has access to a large multiple of global computing power and potentially decades of time.[268] In other words, hash functions enjoy the potential for high security absent dedicated, and resource-intensive, attempts to crack them. Yet, it is not unreasonable to suggest that there may be more efficient approaches for cyber attackers to exploit. Let us delay a brief discussion of this topic until the end of section.

A hash function is *collision resistant* if it is computationally infeasible for an *efficient* adversary to find collisions in the hash functions. Now since all hash functions have collisions, the question is can one efficiently find them? In fact, SHA256 has an infinite number of collisions, and yet no one can find any two binary strings $x \neq x'$ such that SHA256(x)=SHA256(x′). Again, since there are an infinite number of collisions, an attacker can find one by starting to compute SHA256 on the sequence of all binary strings: SHA256(0), SHA256(1), SHA256(00), SHA256(01), etc., until a collision is found. However, because of the pseudo-random property above, we expect the outputs of SHA256 to simulate a uniformly random distribution on the set $\{0,1\}^{256}$, mathematically we expect this approach to take 2^{128} iterations, due to the birthday paradox.[269] Again, assuming even vast

---

267 *See 10 Times More Galaxies!*, NASA, http://nasa.tumblr.com/post/151753781974/10-times-more-galaxies (last visited Nov. 15, 2016) [http://perma.cc/DYN5-XHHQ]; John Carl Villanueva, *How Many Atoms Are There in the Universe?,* UNIVERSE TODAY (Dec. 24, 2015), http://www.universetoday.com/36302/atoms-in-the-universe [http://perma.cc/CUS4-2X2A].

268 Note that in theory an inefficient adversary that had no limits on time, could distinguish the output from random by checking to see if the output sequence results from each possible input string of length 256 bits, by enumerating the output of the above function over all possible binary strings of length 256, and seeing if there is a match. However, this would require an expected 2^{255} attempts, which even by our generous standards of computation, is an astronomical amount of time.

269 The Birthday Paradox comes from the fact that collisions in randomly

computational resources and huge amounts of time, this approach is similarly inefficient.

In both above cases, we can show that brute-force algorithmic approaches could discern a string was not random, or could produce a collision, yet these techniques are inefficient for attackers since they take an astronomically long time. Yet, in both cases one might argue that if one knew specific information about the hash functions, and was clever, then a more efficient algorithm could greatly speed up this process. For example, if we consider the function $g(x)=\lfloor x/2 \rfloor$ again, it is trivial to find collisions: x and x+1 for any even number x are collisions, and it is not at all dependent on the size of the domain or range of the function g. Here, we must note that while it is believed there are algorithms that do better than the brute force approach, they are not believed to do *much* better. That hash functions with these properties can be built is based on beliefs about computational theory, but ultimately these properties cannot be proved outright, as doing so would require solving one of the largest open questions in mathematics, the infamous P vs NP problem.[270]

Cryptographers use a useful heuristic when thinking about cryptographic hash functions such as SHA2, which they call the *Random Oracle Model.*[271] This model is known to be mathematically incorrect in some cases, yet despite this fact it seems to predict hash functions well enough in the cases cryptographers are interested in to be useful without having negative security consequences. [272] In the Random Oracle model, we treat the hash function $SHA256:\{0,1\}^* \rightarrow \{0,1\}^{256}$ as a completely random function with no structure. That is, for each input x, SHA256(x) is chosen to be the result of 256 random coin tosses (where, say, heads represents 0, and tails represents 1). A random oracle of this form is truly random

---

distributed events are much more likely than most people's intuition would suspect. In particular, the probability that anyone in a room of twenty-three people has the same birthday as you is quite low, about six percent, but the probability that *any* two people in such a room share the same birthday is about fifty percent. With just seventy people in the room, the odds of a shared birthday is 99.9 percent. *See* ANTOINE JOUX, ALGORITHMIC CRYPTANALYSIS 185 (2009).

270 The P vs NP problem is considered to be one of the largest open questions in mathematics. It is believed to be unsolvable with current mathematical approaches, has a $1-million-dollar bounty for a solution, is one of the Clay Math Institute's ten Millennium Problems, and is even the focus of a major motion picture. *See generally* LANCE FORTNOW, THE GOLDEN TICKET: P, NP, AND THE SEARCH FOR THE IMPOSSIBLE (2013).

271 *See* DARIO CATALANO ET AL., CONTEMPORARY CRYPTOGRAPHY 137 (2006) (describing the Random Oracle Model).

272 In particular, the model is widely accepted to produce secure results for standard cryptographic protocols, and not one specifically designed to show flaws with the system.

(and thus satisfies the pseudo-randomness property) and collision resistant. For the remainder of this Article, we will treat SHA256 as a random oracle.

Proofs-of-Work

Proofs-of-work are a fundamental technology underlying blockchains. Their basic goal is to allow one party to prove to another that they have spent a certain amount of time working on a given problem, and were invented by Professors Cynthia Dwork and Moni Naor.[273] This may sound abstract and difficult to accomplish, but there is a simple real-world analogy. Suppose we want you to commit so much time to working on something, then one technique is that we can send you a box with a jig-saw puzzle in it, but without a guiding picture, and then ask you, as proof of your work, to send us back a picture of the constructed puzzle. The assembly of the puzzle is something that can be done but it takes effort. The more pieces, the more uniform the picture, and the less hint of what the final picture is, the longer it will take you.

To cryptographically achieve this same concept, we are going to ask you to find the output of a cryptographic hash function with certain properties. In order to ensure freshness, and that you are actually solving work for the request at hand, we will be able to specify a string to the proof; this string is essentially the analogue to the specific picture used for the jigsaw analogy. Thus, if we want a user to proof she's done work with respect to a named string *y,* we will ask that she find us any string x, such that its output begins with i zeros, as shown below:

$$SHA256(y||x) = 0 \quad {}_1 0_2 \dots 0_{\underbrace{i \; zeros}} b_{i+1} \dots b_{256}.$$

Note that in the above example b_j denotes any value of bit. Thus, to complete a proof-of-work on a string y, one iterates through values of x, computing SHA256(y||x) until such time as the output begins with i zeros. Further note that we can vary the amount of work that needs to be done by varying the value *i.* In particular, if we assume the Random Oracle model, then the expectation is that each output bit of SHA256 for a given unique input string y||x is chosen uniformly at random, and thus the probability that such a string begins with i zeros is 2^{-i}. Therefore, to find an appropriate x, we expect to have to iterate through 2^i possible choices. To comprehend this proof,

[273] Cynthia Dwork & Moni Naor, *Pricing via Processing or Combatting Junk Mail*, PROC. OF THE 12TH ANNUAL INT'L CRYPTOLOGY CONF. ON ADVANCES IN CRYPTOLOGY (1993).

.

though, and its implications for blockchain cybersecurity, it is necessary to dive briefly into digital signatures.

Digital Signatures

Digital signatures provide the digital equivalent of a signature for contracts, and include the added security functionality of being non-forgeable.[274] In their simplest form, digital signatures consist of three algorithms, *a key generation algorithm*, a *signing algorithm*, and a *verification algorithm*, (Gen, Sign, Verify) respectively.[275] The signing key may be thought of as the key to a safe that contains a signing stamp. Anyone who has the key can retrieve the signing stamp and use it to "sign" the signature of the individual whose name is on the stamp; hence the need to keep it secret.

The signing algorithm takes a message M, and a singing key SignKey, and generates a signature σ, denoted $\sigma \leftarrow$ Sign(SignKey,M). Extending our analogy, this corresponds to using the key to unlock the safe and to stamp the document containing the message. Unlike this analogy, though, the signature produced is a string that binds the specific message M to the signing key, such that only someone with the verification key can check that that the signer did in fact sign the message. It is computationally infeasible for anyone not possessing the Signing Key to forge a signature and come up with a new signature σ′, regardless of how many pairs of valid signature message pairs (M_i,σ_i) they have seen.

The verification algorithm takes a message M, verification key VerifyKey, and a signature σ, and returns *true* if the signature σ truly was generated by applying the Signing algorithm with the message M, and the appropriate signing key, SignKey, (i.e., $\sigma \leftarrow$Sign(SignKey,M)), and *false* otherwise. It is used for verification, with significant applications for the peer-to-peer networks at the heart of blockchains.

Peer-to-Peer (P2P) Network

Peer-to-peer networks, while not cryptographic, are a key component of modern blockchains. A peer-to-peer (P2P) network is simply an overlay network on the Internet in which there is no central authority that regulates it, and where clients of the network communicate directly with one another. Despite the lack of central coordination, the network provides

---

274 *See* Electronic Signatures in Global and National Commerce Act (ESIGN), Pub. L. 106–229, 114 Stat. 464, enacted June 30, 2000, 15 U.S.C. ch. 96.

275 *See* JOSÉ LUIS GÓMEZ PARDO, INTRODUCTION TO CRYPTOGRAPHY WITH MAPLE 538 (2012).

services that appear to come from a singular source. Thus each computer on the network has both client and host functions.[276] Popular examples of P2P networks include the BitTorrent file sharing protocol, which allows people to transfer files to and from other computers on the network without a centralized authority having a list of all the participants or available files.[277] Such networks became popularized after the initial file sharing network Napster was taken down, resulting in the rise of various P2P networks that have proven largely immune to attempts to disable them, with the Silk Road saga being a case in point.[278]

---

[276] *See* CHWAN-HWA (JOHN) WU & J. DAVID IRWIN, INTRODUCTION TO COMPUTER NETWORKS AND CYBERSECURITY 188 (2016).

[277] *See* JONAS ANDERSSON SCHWARZ, ONLINE FILE SHARING: INNOVATIONS IN MEDIA CONSUMPTION 132 (2013).

[278] *See, e.g.*, Patrick Howell O'Neill, *Meet OpenBazaar, the Black Market That's Part Silk Road and Part eBay*, DAILY DOT (Nov. 7, 2014 4:38 AM), http://www.dailydot.com/layer8/openbazaar-is-next-after-silk-road-2-falls/ [https://perma.cc/8MPW-TPT2].