ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

A Policymaker's Guide to Blockchain

ALAN MCQUINN AND DANIEL CASTRO | APRIL 2019

Policymakers can and should do more to support blockchain innovation and adoption, such as ensuring regulations are targeted and flexible, so as to encourage blockchain experimentation.

KEY TAKEAWAYS

- Blockchain is a powerful new technology that creates a distributed digital ledger that allows multiple parties to engage in secure, trusted transactions with one another without an intermediary.
- Blockchain is best suited for certain types of applications, including cryptocurrencies, shared data services, smart contracts applications, decentralized marketplaces, authenticity tracking, and digital identity.
- Governments can and should do more to support blockchain innovation and adoption, including by supporting public sector adoption, creating a flexible regulatory environment to allow experimentation, and using targeted regulatory enforcement.

INTRODUCTION

The Internet era has enabled many types of transactions to become digital, such as financial deposits and withdrawals, but records of these transactions are still maintained by a centralized gatekeeping organization, such as a bank. Blockchain is a powerful new technology that creates a distributed digital ledger—a database—that allows multiple parties to engage in secure, trusted transactions with one another without an intermediary. For example, blockchain has enabled the creation of "cryptocurrencies," which are digital currencies created without a central monetary authority people can use to send money electronically, without banks. However, blockchain has many other uses that create opportunities for both public and private organizations to boost productivity, open new markets, and disrupt legacy business models. Policymakers should accelerate the adoption of blockchain by promoting government use of the technology and modernizing regulations to ensure policy does not hold back positive uses of the technology.

In 2009, "Satoshi Nakamoto," the pseudonym for an as-yet unidentified individual or group of individuals, released the code for the first blockchain system in order to create the peer-to-peer virtual currency Bitcoin.[1] Bitcoin's blockchain architecture, for the first time, eliminated a fundamental problem with distributed payment systems by making it impractical for any participant to defraud the system by spending the same unit of virtual currency more than once. It worked by combining several advanced cryptographic techniques and an incentive structure that ensured participants would work together without needing to trust one another. While Bitcoin still has relevance today as a form of cryptocurrency, many individuals, companies, nonprofits, universities, and governments have borrowed code or ideas from Bitcoin's blockchain system to create entirely new and innovative blockchain applications to tackle myriad challenges. In particular, organizations are using blockchain to enable a network of actors to conduct trusted transactions without a central authority.

Over the last decade, there has been a frenzy of investment in different digital currencies, various types of blockchains, and unique services based on blockchains and digital currencies. Technology companies, such as IBM, have offered blockchain-as-a-service applications, while financial services providers such as Scotiabank, Danske Bank, and US Bancorp have invested in a shared blockchain.[2] Moreover, many start-ups have used blockchains to raise capital by selling digital tokens to investors as an alternative to traditional venture capital funding or initial public offerings. But importantly, much of the coming wave of blockchain applications will be outside the financial industry.

Blockchain has received significant media attention over the past few years, driven both by the astronomical profits of early investors in Bitcoin and the outlandish claims by some that the technology may fundamentally alter society, national sovereignty, and democracy. Like the Internet frenzy in the early 2000s, the high level of attention has inspired many organizations to jump on the blockchain bandwagon—in 2018, for example, after an iced tea company changed its name to include the word "blockchain," its stock increased by 500 percent.[3] Regulators have

been slow to police blockchain activities, thereby creating opportunities for criminals to launder money and defraud investors. These practices have come under the scrutiny of several financial regulators.[4]

Nevertheless, a rich ecosystem of legitimate blockchain-based projects has emerged, and the coming years will likely see many new applications using blockchain, and greater adoption of new and existing applications such as tracking goods in global supply chains and enabling peer-to-peer transactions between connected devices. For example, a 2018 report from the World Economic Forum and Bain & Company estimated that by deploying blockchain, global businesses could generate an extra $1 trillion in trade finance (lending for importers and exporters) than otherwise would be generated.[5]

However, governments can and should do more to support legitimate blockchain innovation and adoption, including ensuring regulations do not unnecessarily limit certain blockchain-based applications. Toward that end, this report offers 10 principles to guide policymakers as they approach this task:

1. Ensure technology neutrality.
2. Actively support blockchain adoption and deployment in the public sector.
3. Support blockchain research and development.
4. Promote legal certainty for blockchain applications.
5. Set rules for blockchains at the national, not subnational, level.
6. Create a flexible regulatory environment that enables experimentation.
7. Use targeted regulatory enforcement to incentivize companies to protect consumers.
8. Avoid laws and regulations that prevent the use of blockchain technology.
9. Promote data interoperability for blockchain applications.
10. Work to establish international harmonization of blockchain regulations across sectors.

WHAT PROBLEM DOES BLOCKCHAIN SOLVE?

Blockchain solves a problem that far predates its creation: how to get a group of actors to reach consensus despite not being able to trust one another. The problem, known as the Byzantine Generals' Problem, originally described a group of generals, each commanding part of an army and separated by distance, having to reach consensus as a group whether to attack or retreat all at once, because their entire combined forces would suffer a defeat if only some of them attack or retreat.[6] Unfortunately, the generals cannot trust one another, and the messengers they use to communicate may be traitors or spies.

Many processes use a trusted intermediary, such as a business or government agency, to coordinate activity among multiple parties engaged in related transactions. These intermediaries often provide many functions, one of which is creating and maintaining a system of record to provide an authoritative source of information about transactions, which all parties rely on to be accurate. For example, banks keep records about transfers of funds between customers; deed registries maintain official records on land ownership from buyers and sellers; and government agencies maintain official records on births and deaths of its citizens. Before blockchain, it was not feasible for the parties involved in these transactions to also be responsible for maintaining the authoritative records of these transactions because of the potential for committing fraud or introducing other errors into these records. Imagine, for example, the problems that might arise if bank customers could independently modify the official records of their history of deposits, withdrawals, and check payments.

Blockchain eliminates the need for a trusted intermediary to maintain an official system of record by creating a distributed digital ledger with which all parties can verify they have access to the exact same data and no party is able to make unauthorized alterations of existing records. Because all parties can have their own copies of the data, blockchain increases transparency, enables auditing, and eliminates any single points of failure. These features come at a cost, however, as blockchain involves many different computer systems duplicating the same data and engaging in redundant computing tasks.

Blockchain offers many important benefits when there is no existing intermediary, existing intermediaries are costly or unreliable, or existing intermediaries can use blockchain to efficiently increase the transparency, security, or reliability of their records.

Because blockchain eliminates a key role for trusted intermediaries (i.e., maintaining a system of record), many blockchain enthusiasts posit that the technology has the potential to significantly disrupt existing processes and organizations, thereby bringing new levels of efficiency to transactions. In particular, blockchain allows actors to move away from depending on a centralized or hierarchical organizational model to a decentralized one. Obviously, this potential for disruption depends on many different factors, as intermediaries may provide many more important functions beyond a system of record, including validating or verifying details about a transaction in the real world.

Still, blockchain offers many important benefits when there is no existing intermediary (such as when the government or private sector is not providing a needed service); existing intermediaries are costly, cumbersome, or unreliable; or existing intermediaries can use blockchain to efficiently

increase the transparency, security, or reliability of their records. Moreover, because blockchain technology continues to improve, the costs associated with running a large decentralized database will likely decline, which will make it more viable for different use cases.

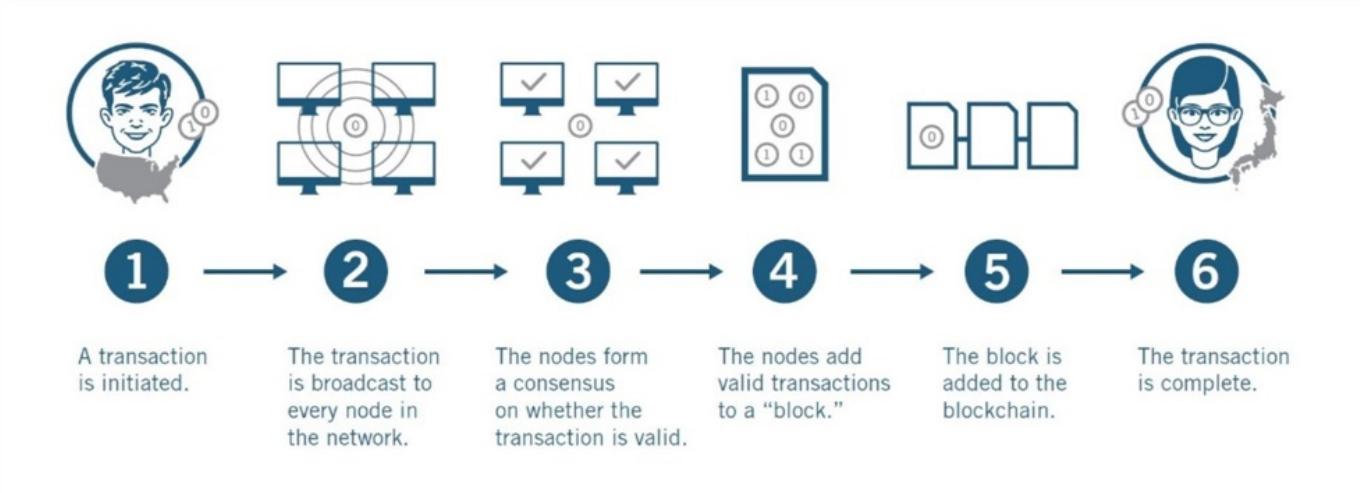
WHAT IS A BLOCKCHAIN AND HOW DOES IT WORK?

Blockchains are digital ledgers that record information that is distributed among a network of computers that ensure each computer has identical records. Blockchain technologies consist of three fundamental components: cryptographically linked data structures, peer-to-peer networking, and consensus protocols.

First, the blockchain consists of a series of digital "blocks" that are securely linked together in sequential order using cryptography to create a virtual chain of data. These blocks record information such as financial transactions, agreements between parties, and ownership records (see figure 1).

Second, blockchain runs on a distributed peer-to-peer network of computers. Each computer in the network, referred to as a node, stores a copy of the blockchain, validates that the blockchain has not been tampered with, and verifies when transactions can be added to a new block. Nodes share and synchronize all updates.

Figure 1: How a Blockchain Works



Finally, blockchains maintain agreement between all participants using a "consensus protocol"—a set of rules that allows nodes to determine when to add new information to the blockchain. Consensus protocols are designed to make the blockchain resistant to tampering and ensure consistency in the data among all participants in the network.

There are many types of consensus protocols that use different techniques, each with various benefits and drawbacks. This report will briefly describe five: proof of work, proof of stake, practical byzantine fault tolerance, proof of elapsed time, and proof of burn (see table 1).

Table 1: Consensus Protocols and their Strengths and Weaknesses

Consensus Protocol	Strengths	Weaknesses	Examples
Proof of Work	Highly tamper-resistant, redundant, and transparent	Energy-intensive, difficult to scale, difficult to make corrections	Bitcoin and Ethereum
Proof of Stake	Energy efficient, faster transactions, scalable	System naturally disadvantages small nodes, difficult to make corrections	Peercoin, Tezos, and Qora
Practice Byzantine Fault Tolerance	Energy efficient, faster transactions, scalable, editable, removes incentive structures	Limits number of participants, less redundancy, and less tamper resistance	Linux Foundation's Hyperledger
Proof of Elapsed Time	Energy efficient, removes incentive structures, scalable	Requires specific hardware	Intel's Software Guard Extensions, and Hyperledger Sawtooth
Proof of Burn	Enables value creation for one blockchain using another, energy efficient	Requires destroying value created by other cryptographic assets, difficult to scale, difficult to make corrections	Slimecoin and Counterparty

Proof of Work

The most popular consensus mechanism, known as proof of work, requires nodes in the network to compete to solve complex cryptographic puzzles before a new block can be added. Solving these puzzles is computationally complex, requiring nodes to engage in a certain amount of work. The parameters of each puzzle are periodically updated to ensure it takes a certain amount of time to solve them. Nodes in cryptocurrency blockchains with proof-of-work consensus mechanisms are called "miners" because the blockchain system rewards the node that is first to solve the problem and create a new block with cryptocurrency.

However, while it is difficult to solve these puzzles, verifying that the puzzle has been solved is computationally simple.[7] This is done through what is called a hash function, which generates a unique digital fingerprint for any given piece of data. Even a slight modification of the input will result in a dramatically different hash output. Hashing is a one-way function, meaning it cannot be reversed. Therefore, this process makes it easy to verify transactions, but difficult to fake them. When a miner confirms a block as valid, it creates two hashes: a hash of every transaction in the block, and a hash proving it has solved the previous cryptographic puzzle.[8] Because each block includes the hash with information about the previous block in the chain, nodes cannot retroactively modify a block without first solving the cryptographic puzzle for that block and every block after it—a task that is too difficult for any node to accomplish on its own.

Blockchains with proof-of-work consensus mechanisms are energy intensive, which makes them difficult to scale. For example, the Bitcoin and Ethereum blockchains consumed roughly 75 terawatt-hours of electricity in 2018.[9] While this is less than 0.4 percent of global annual electricity usage, it is more than some countries—Portugal, for example, consumes roughly 49 terawatt-hours annually.[10] However, much of this energy consumption takes place in data centers in countries such as China because energy there is cheap, but, unfortunately, mostly produced from fuels with high carbon emissions, such as coal.[11] The energy consumption patterns will likely evolve over time as blockchains use different consensus mechanisms that are less energy intensive, or as the economics of mining change.

BOX 1: BLOCKCHAIN SECURITY RISKS

While some types of blockchains, such as proof-of-work models, are highly tamper resistant, attackers have successfully used several methods to undermine the security of blockchain-based applications.

Poor Implementations, Bugs, and Glitches

Developers can make coding mistakes when creating new blockchain software.[12] For example, developers helping to maintain the Bitcoin network discovered a bug in 2018 that would have allowed attackers to create new bitcoins and inflate the supply of currency.[13] Similarly, the developers of the cryptocurrency Zcash found a flaw in its underlying cryptography in February 2019 that malicious parties could exploit to generate unlimited currency.[14]

Attacks on Peer-to-Peer Networks

An "eclipse attack" occurs when an attacker isolates a specific user from the decentralized network to fool the network into accepting fake information, and then confirming fraudulent transactions.[15]

Attacks on Consensus Protocol

A "51 percent attack" occurs on a proof-of-work blockchain when a group of bad actors installs more mining capacity than the rest of the network, enabling them to retroactively make changes to the digital ledger.[16] For example, in May of 2018, the cryptocurrency Bitcoin Gold suffered a 51 percent attack that resulted in the theft of $18 million worth of the previously 26th-largest cryptocurrency.[17]

Attacks on Applications Using Blockchain

Attacks can target software that uses blockchain. For example, in 2014, a group of hackers stole millions of dollars of bitcoins from a cryptocurrency exchange called Mt Gox due to poor security in that company's systems.[18]

Proof of Stake

In proof-of-stake consensus mechanisms, the system chooses each creator of a new block in a deterministic way based on the "stake" they control in the blockchain.[19] Each node is linked to an address where tokens are stored, and the more tokens each has (i.e., the node's stake in the system) the higher the chance that node has of being able to validate the next block. For example, if one node has 50 tokens and another node has 100 tokens, the latter node is twice as likely to be able to validate the next block in the chain. Rather than give tokens for validating a block, the system rewards nodes in the form of transaction fees from users. This type of consensus mechanism is more efficient than the proof-of-work model and works best when there is a static supply of tokens.

One problem with proof-of-stake models is holders with small numbers of tokens are very unlikely to "win the lottery" and generate a block. This creates a disincentive for participants with low token balances to run a node, which is bad for the database overall because the more participants in a blockchain, the more secure it is.

To solve this problem, developers have created two variants of proof of stake. First, in leased proof-of-stake models, nodes can lease their account balances to one another to create a higher chance of generating a block. Participating nodes remain in control of their tokens and can spend them at any time. Second, in delegated proof-of-stake models, token holders use their balance to elect a list of nodes that have the chance to generate a block. While these participants do not receive rewards in the same way as other proof-of-work models, they can vote on changes to the database parameters, and have greater ownership and influence over the blockchain.

Practical Byzantine Fault Tolerance

Predating the Bitcoin blockchain, the MIT Laboratory for Computer Science created practical Byzantine Fault Tolerance (PBFT) in 1999 to solve the Byzantine Generals' problem.[20] Since that time, several blockchain projects have incorporated PBFT into their consensus mechanism, including the Linux Foundation's Hyperledger.[21]

PBFT is a very complex process that works by ordering all nodes into a sequence wherein the primary node, or the leader, is followed by the other backup nodes.[22] All of the nodes maintain an internal state (i.e., ongoing specific information), and communicate with one another frequently. When a node receives a message, it uses the message in conjunction with its internal state to run a computation or operation, which informs that individual node what to think about the message. Then, after reaching its conclusion about the new message, that node shares its decision with all the other nodes in the system. By doing this, nodes not only have to prove that messages came from a specific peer node, but also need to verify that the message was not modified during

transmission. The final result occurs when all honest nodes come to an agreement on the order of the record and either accept or reject it. The primary node sends out each request multiple times and directs this process in a round-robin style.

PBFT has several advantages and disadvantages.[23] PBFT both requires less energy than in proof-of-work models and enables nodes to easily validate and confirm a block. However, PBFT only works well when there is a relatively small consensus group, because it requires a significant amount of communication from all nodes to achieve consensus. Therefore, these blockchains are often more centralized and permissioned. PBFT models are also susceptible to attacks wherein a single party controls many nodes in the network—the dangers of which are often mitigated by having larger networks not supported by this model.

Proof of Elapsed Time

Proof of elapsed time is a consensus mechanism that includes a fair lottery system wherein every node is equally likely to be a winner and create a block. In proof-of-elapsed-time models, each node generates a random wait time and goes to sleep for that duration. The node that "wakes up" first creates a new block for the blockchain, broadcasting the necessary information to the whole network. Intel created this alternative protocol in 2016 as a solution to "random leader election," and completely operates the protocol.[24] The system is designed to use a trusted execution environment, which ensures all participating nodes generate and complete random wait times. This type of consensus mechanism is one of the most energy efficient, but requires users to have specialized hardware and place their trust in the software developers that fully control the consensus mechanism.

Proof of Burn

In a proof-of-burn consensus mechanism, nodes must show proof that they have "burned" other cryptocurrencies—by sending them to a verifiable address where they cannot be spent (also known as the eater address)—in order to grant the node rights to generate a block.[25] This process, unlike proof of work, does not consume any resources other than the burned tokens, which are removed from circulation. Once the system verifies the tokens can no longer be used, it rewards nodes with tokens. Developers have only implemented this type of consensus protocol a handful of times because it requires permanently removing assets.[26] However, it does enable developers to bootstrap one cryptocurrency off another.

Public vs Private Blockchains

There are primarily two types of blockchains: public and private. A public blockchain is open: Any participant in the network can read, send and receive transactions, and partake in the consensus process as a node. Public blockchains operate using "cryptoeconomics," the combination of economic incentives and cryptographic verification, such as with proof of work.[27] After public blockchains are set into motion by developers, volunteers join the peer-to-peer network. In public

blockchains, such as Bitcoin, consensus mechanisms push the responsibility of security to the individual computers operated by the users. For example, the individual owner is responsible for securing the private key that corresponds to each bitcoin, for without it, the user cannot spend those bitcoins. Moreover, no intermediary, such as a credit card company, could intervene and control the ledger to reverse fraudulent transactions.

In a private blockchain, also known as a permissioned blockchain, the operator places restrictions on whom can participate and what transactions they can access and conduct. Private blockchains can be formed by a consortium wherein each blockchain is operated by a preselected number of nodes that correspond to private entities such as banks, or be wholly private, with permissions controlled by one organization. In the latter, the organization determines who can access and read a private blockchain or participate as a node, depending on the application. These applications tend to be more centralized than public blockchains and use blockchains to improve auditability. In addition to single-entity and consortium blockchains, there are semi-private blockchains, which are run by a single entity that grants access to any user who qualifies for access.

Public and private blockchains each have their own strengths and weaknesses.

Table 2: Public Versus Private Blockchains

	Strengths	Weaknesses
Public Blockchains	Easier to start, transparent, redundant, more tamper resistant	Difficult to make changes, govern, or scale
Private Blockchains	Easier to edit and govern, more scalable, and enable privacy	Less redundancy and tamper resistance, more difficult to start

Public blockchains are typically easier to start, more transparent, and offer more redundancy. To start a public blockchain, developers simply release code and encourage people to join the network as nodes. In addition, public blockchains tend to be completely transparent, with any participant able to read the public blockchain and track transactions over it. Moreover, by having a diffuse and decentralized user base of nodes, the network becomes very redundant, such that any node can double-check new blocks to ensure no faulty transactions have been added into the system. Finally, public blockchains are often highly resistant to tampering. The enormous amount of computing power participating in public proof-of-work blockchains, such as Bitcoin, make it nearly impossible for bad nodes to make false transactions.

However, compared with private blockchains, it is harder to make changes to the software or ledger in public blockchains, even when major errors occur. Perhaps the most famous example of this was the exploit that targeted Ethereum's blockchain in June 2016. A user found a coding loophole in a smart contract—programs that encode certain conditions and outcomes so the outcomes happen automatically—that allowed them to drain value from other investors in a way that was not intentional yet allowed under Ethereum's terms and conditions.[28] Ethereum's

developers quickly created a patch to prevent this bad actor from withdrawing the stolen Ether (the blockchain's currency), which was strongly supported by Ethereum's founder and several community leaders, but because the update could not be enforced on the public blockchain, a minority of Ethereum users did not update their software and continued the blockchain under its original rules, now called "Ethereum Classic."[29] This resulted in a "fork," wherein the public blockchain split into two different blockchains operating under separate software versions (see box 2).

BOX 2: WHAT IS A FORK?

In software development, a fork occurs when developers take a copy of code from one project and make changes to it for a new project, thereby creating two different projects with the same base code. Similarly, in public blockchains, a fork occurs when some participants change some aspect of the blockchain's code while others do not. This disagreement, whether intentional or not, results in multiple versions of that blockchain. There are two types of forks.

Soft Forks

Soft forks, or accidental forks, occur when updates are not compatible. Nodes using different versions of the software create two different ledgers—one from the older version and one from the newer version. Non-upgraded nodes still see new transactions as valid, but transactions from non-upgraded nodes are rejected by the upgraded nodes.

Hard Forks

Hard forks occur when a blockchain's developers decide to update the software so that older versions will not be compatible with newer versions. Transactions from nodes that continue to run the old software will be invalid, forcing all nodes to upgrade to the new rules.

Moreover, current public blockchains—most of which are run through proof-of-work consensus protocols—are resource intensive and difficult to scale. For example, the slow rate of block verification on the Bitcoin blockchain means the system can only handle five to seven transactions per second.[30] Ethereum can handle only 15 transactions per second (although there are plans to switch to a proof-of-work system that can handle a million transactions per second).[31] This number is tiny compared with Visa's global credit card network, which is capable of processing 56,000 transactions per second as of 2014.[32] (Although, in reality, Visa's system only averages a fraction of that: roughly 1,700 transaction per second as of 2016.[33])

By contrast, private blockchains can enable more privacy, greater scalability, and faster, cheaper transaction clearing. With fewer nodes, less-strenuous consensus mechanisms, and signed contracts between entities, private blockchains have greater leeway to generate efficiencies, and can choose what information is accessible to participants on the ledger. Moreover, private, permissioned blockchains can achieve easier consensus to update the system or retroactively edit transactions. Accenture, for instance, created an "editable blockchain" in 2016.[34] Indeed, certain types of private blockchains can use a technique called a "chameleon hash function" to make efficient and transparent changes to specific transactions without risking a fork to the system.[35] By the same measure, the weaknesses of private blockchains are the strengths of their public counterparts. Indeed, permissioned blockchains often lack the same transparency, redundancy, and tamper-resistant nature of the public blockchains.

BLOCKCHAIN APPLICATIONS

A rich ecosystem of blockchain-based projects has emerged and continues to grow as both the public and private sector explore new applications for which this technology proves most fruitful. While some blockchain applications are maturing, others are still in their nascent stages as researchers seek to improve blockchain systems to address problems such as scalability and efficiency.

Simply converting most applications to run on a blockchain would not necessarily add value, and in fact would likely be inefficient and costly.

Since blockchain is a database, almost any database application could be run on one. However, converting most applications to run on a blockchain would not necessarily add any value, and in fact would likely be inefficient and costly. Successful blockchain-based applications generally share a few elements. For example, blockchain applications typically involve multiple parties that need to access and make entries in the database but may not trust one another, because, for example, they do not know the others' identity or because they have conflicting interests. Because blockchain establishes a permanent record of transactions, it is also used in cases wherein auditability is important. And because blockchain involves a distributed database, it is also useful in cases in which it is helpful for different stakeholders to have a copy of the authoritative set of records.

Public and private blockchains are appropriate for different scenarios. For example, if a group of entities want to control access and functionality on a blockchain, but still need to achieve consensus, they may want to use a private consortium model. However, if entities want anyone to participate, ensure the network has redundancy and public transactions, they may want a public blockchain.

Blockchain will likely have the most impact in six applications: cryptocurrencies, shared data services, smart contracts applications, decentralized marketplaces, authenticity tracking, and digital identity applications. Certainly, some applications overlap between different categories. For example, supply chain management applications have elements of shared data services and authenticity programs, as they are designed to track and authenticate real-world goods, but also serve as a large repository of data for all users to access, amend, and analyze.

In each of these areas, it is important to distinguish between the benefits from digitization versus those from using blockchain. For example, digitizing property records enables buyers and sellers to radically improve the efficiency of title searches and insurance. Similarly, providing citizens with electronic identification enables more efficient e-commerce transactions and facilitates e-government services. While blockchain can be used for these applications, many of the most important benefits arise from digitization rather than from blockchain. Policymakers should therefore strongly support efforts to increase digitization but be neutral as to what technology is best suited for particular applications.

Cryptocurrencies

Over the last decade, many entities in both the public and private sectors have devoted resources into creating digital units of exchange called virtual currencies. While physical currencies use paper and metal (i.e., bills and coins) to represent information, virtual currencies exist purely in electronic form. A virtual currency can either be issued by a central authority or generated in a decentralized network wherein no single entity controls its functions. Blockchains have enabled the most popular type of virtual currency, called cryptocurrencies, which use cryptographic techniques to regulate and decentralize the creation of units of currency and verify the transfer of funds. While most cryptocurrencies are not backed by a government, some national governments, such as Canada and China, have started to develop them.[36] Moreover, Venezuela has launched its "Petro" cryptocurrency, which is backed by its oil reserves, although the currency's value remains uncertain.[37]

Cryptocurrencies use public-key cryptography. Users have both a public and a private key. The public key may be shared with anyone, and others can use it to send someone cryptocurrency only the holder of the corresponding private key may access. These systems allow for one-on-one transactions to occur between people who had no previous interaction. When users want to exchange cryptocurrency for products or services, they can use a digital wallet service to send and receive digital currency or exchange it for fiat currency—legal tender backed by a government.[38] When users want to trade cryptocurrency for fiat currency, they do so on online platforms called cryptocurrency exchanges. Cryptocurrency exchanges are either brokers for exchanging currencies directly, such as a currency exchange at the airport, or intermediaries that allow users to trade currencies with one another—at either a fixed price set by the exchange or market prices set by the sellers themselves.

Bitcoin is the first and most prominent example of a cryptocurrency.[39] The second most popular cryptocurrency is Ethereum, which focuses on running the programming code of decentralized

applications (see Smart Contracts section). Both Bitcoin and Ethereum currently use proof-of-work consensus protocols and together represent roughly 60 percent of the total cryptocurrency market capitalization.[40] There are hundreds of other active cryptocurrencies. In fact, one list says there were roughly 2,000 cryptocurrencies available as of February 2019.[41] These cryptocurrencies have many contributors across a diverse community of entrepreneurs, software developers, and other users.

Cryptocurrencies have many benefits in terms of privacy, low-cost transactions, and global reach.[42] First, because many digital currencies do not require personal identifying information, unless users choose to publish their transactions, they will remain pseudonymous (associated only with their public key). Second, digital currencies have relatively small fees associated with processing transactions. For example, Bitcoin transaction fees average roughly $0.30 per transaction (as of February 2019), which is significantly lower than credit card fees that can range from 0.5 to 5.0 percent of a transaction, plus $0.20 to $0.30.[43] Third, users of digital currencies can quickly send payments at any time to anywhere in the world using blockchain technology. For example, software developer Ripple Labs, creator of the cryptocurrency XRP, uses its RippleNet blockchain to allow financial institutions to send money anywhere in the world and settle those payments instantly.[44]

But while the primary purpose of cryptocurrencies is to function as a unit of exchange, many now use them for speculation, built all too often on the "greater fool theory"—the idea that the price of something is determined by the irrational beliefs and expectations of market participants rather than its intrinsic value. The value of most decentralized currencies is highly volatile due to their relatively small market size (i.e., because the price is determined by supply and demand, it takes a smaller amount of money to affect the price of a virtual currency than a fiat currency), which generates uncertainty among the businesses and users that adopt them.[45] Couple that with the fact that speculators can mint their own currencies by engaging in mining, it is not surprising users primarily buy cryptocurrencies as an investment. This is especially true for individuals in countries with highly volatile fiat currencies.

There are several challenges associated with the adoption and deployment of cryptocurrencies, in addition to those of public blockchain applications generally. First, cryptocurrencies are vulnerable to misuse for criminal activities, such as money laundering, criminal funding, and malware, because there is little regulation and enforcement. Under-enforcement of anti-money laundering regulations appears to have precipitated the rise in criminal activity. This trend is especially troubling given the rise of truly private coins (discussed later in this report). However, illegal activities are easy to track on public blockchains. For example, *The Wall Street Journal* recently discovered nearly $90 million in suspected criminal proceeds that went through one online cryptocurrency exchange over a two-year period.[46]

Second, investors in the cryptocurrency industry have been susceptible to fraud. Some fraudsters have used cryptocurrencies to launch Ponzi schemes, in which the success of a nonexistent enterprise is stimulated through quick returns for first investors using money invested by later investors. For example, in March 2019, the New York attorney general arrested the developers of

OneCoin for allegedly defrauding investors through a Ponzi scheme that made $3.7 billion in revenue.[47] Similarly, a number of companies used bogus business plans for their initial coin offerings (ICOs) (see box 3). In fact, a study from 2017 found that approximately 80 percent of the ICOs it analyzed were scams.[48] As a result, the practice has come under the scrutiny of several regulators, with the U.S. Securities and Exchange Commission (SEC) launching several investigations into fraudulent ICOs.[49]

BOX 3: WHAT IS AN INITIAL COIN OFFERING?

Some companies use ICOs as an alternative to raising funds from venture capital or initial public offerings.

In an ICO, rather than buying an ownership stake in a company, investors buy into a new virtual currency they expect will increase in value based on that company's proposed business model. Usually, a company releases a document that details how the system works and asks for investors to finance the business in exchange for a new coin. Investors then hope these coins are used a lot, which raises their value.

In an ICO, companies can offer two types of "coins": securities and utility tokens.

Securities

The majority of tokens sold in ICOs are securities. Securities are a broad classification that refers to any kind of tradable asset. These tokens can be backed by anything from precious metals to real estate. There is a four-part test to determine whether a token is a security[50]:

1. Is the token an investment of money?
2. Is it placed in a common enterprise?
3. Does the investor expect profits?
4. Are those profits derived from the effort of others? The Security and Exchange Commission (SEC) oversees securities.

Utility Tokens

Some tokens may not strictly meet the four requirements of securities. These "utility tokens" are designed for a specific application, such as to provide users with access to a product or service. For example, Filecoin raised money using an ICO, but tokens sold via this offering can only be used to purchase decentralized cloud storage once the service has launched. SEC still treats these token sales as securities primarily because they often incorporate securities features or are marketed as having a potential for profit. However, SEC has not ruled out future utility coin offerings not fitting the criteria of securities.[51]

Third, cryptocurrencies are susceptible to manipulation, which increases their volatility. For example, automatic trading programs, also called bots, appear to be engaging in effective price manipulation for Bitcoin and other cryptocurrencies.[52] In a 2019 report before SEC, the asset management company Bitwise found nearly 95 percent of reported trading in Bitcoin from 81 exchanges had been created through artificial trading.[53] And while these bots exist legally in other established markets, such as the New York Stock Exchange, exchanges of cryptocurrencies often lack the same level of oversight for abusive and illegal activities as their more established counterparts.[54] This is one reason the Commodities Futures Tradition Commission (CFTC) and the office of the New York attorney general are investigating currency manipulations.[55]

Finally, it is unlikely there will ever be a truly effective global currency, as currency valuations need to reflect changes in the underlying global competitiveness of national economies. To see the problem of global currencies, one only need look at the European Union, where a single currency has made some member states no longer price competitive in the global market, while making others more competitive.[56] This does not mean governments could not eventually use digital currencies as fiat money, but that is not likely to happen in the near term.

Case Study: Stablecoins

Cryptocurrencies are known for their volatility. For example, in June 2018, the price of bitcoin jumped from around $5,900 to around $8,200, much lower than its high point of $19,511 in mid-December 2017.[57] To combat this instability, some entrepreneurs have attempted to peg their cryptocurrency to the dollar or other real-world assets. These cryptocurrencies, called stablecoins, rely on real-world assets or a combination of game theory and trading bots to ensure a cryptocurrency is pegged to the value of a real-world asset.[58] Unfortunately, the pegs of these coins often fail to be stable. Indeed, these coins only work effectively if they are always convertible to the asset to which they are pegged. Without convertibility, there can be no parity.[59]

There are three types of stablecoins. First, some stablecoin developers believe they can peg their cryptocurrency by acting like a "central bank."[60] In this process, developers control a cryptocurrency and then use algorithms to artificially manipulate either the supply of the cryptocurrency or the supply of pools of cryptocurrency collateral to "back" the coin against a real-world asset. Similar to such countries as Zimbabwe and Venezuela, which overstate the value of their currencies, as compared with actual market exchange rates, the price of this type of stablecoin is artificially set by its developers rather than the free market. As such, these schemes often fail. For example, in 2014, the Bitshares project tried to use this method to peg its stablecoin, BitUSD, to the U.S. dollar. The project failed to hold its peg after the first 100 hours.[61] Second, developers can try to peg their stablecoins to the value of a real-world asset using other cryptocurrency as collateral. For example, the company Maker has a stablecoin called

Dai that is backed by Ethereum held as collateral in an Ethereum smart contract.[62] Unfortunately, these systems often over-collateralize the cryptocurrencies, and are subject to fluctuations due to volatility in the underlying cryptocurrency.[63]

Finally, stablecoins can be backed by real assets. For example, the Gemini Dollar is redeemable one for one with an actual dollar held in a trust company or actual bank.[64] This type of stablecoin has convertibility and parity.[65] Given proper regulatory compliance, this type of cryptocurrency could reduce costs, remove intermediaries, and automate and improve transparency for certain financial transactions—especially in countries with a volatile fiat currency that do not have easy access to such stable assets as the U.S. dollar.[66] Indeed, six banks have announced their intention to issue their own stablecoins over the IBM global payment network.[67]

Regulators have recently started to scrutinize stablecoins, although they have taken few regulatory actions to date. For example, representatives from SEC have said some stablecoins—particularly those that rely on some sort of pricing mechanism to maintain their peg—may be securities under U.S. law.[68]

Case Study: Privacy Coins

For the most part, transactions over public blockchains are pseudonymous rather than private. Any member of the network can verify the ledger of a public blockchain by checking the transactions and hashes all the way back to the start of the blockchain. Users have full transparency into the network, can track transactions, and are able to see how much cryptocurrency is in anyone's public wallet, but they need additional information from an outside source to link an account to an individual. Therefore, while public cryptocurrencies can facilitate illicit activity, they also offer law enforcement useful tools for tracking down criminals. For example, the Federal Bureau of Investigations was able to easily seize the bitcoin earnings of the operator of Silk Road—an infamous online marketplace for illegal goods and services—because of the public transaction record.[69]

However, certain cryptocurrencies, called "privacy coins," offer users true anonymity and therefore have a high risk of being used for criminal activity. These cryptocurrencies utilize cryptographical features to obfuscate transactions and make them more difficult to track while still enabling consensus.[70] For example, "zero-knowledge proofs" are a method by which one party can authenticate information without actually conveying that information.[71] While privacy coins use a public blockchain for transactions, the sender and receiver of a transaction are obscured which prevents the activity from being tracked. The cryptocurrency Monero, for example, operates on a proof-of-work blockchain that enables users to send transactions, but no outside observer can tell the sender, destination, or the amount of transaction.[72] This cryptocurrency has already been involved in illicit activity, when the operator of the WannaCry ransomware attack moved funds from Bitcoin to Monero.[73]

Shared Data Services

Some applications use blockchain ledgers to create a repository of data users can access, add to, and extract insights from. With blockchain-based models, many different entities that may have conflicting interests can contribute to a shared database knowing their shared ledger will be accurate. For example, 100 financial institutions have signed up to a blockchain consortium created by the company R3, which will allow them to share information regarding trade finance (lending for importers and exporters).[74] Importantly, these businesses often compete for the same business or have conflicting interests within a supply chain. In this new system, there is no trusted intermediary, such as a third party or government agency, to coordinate the activity between participating entities—financial services companies, importers and exporters, shipping companies, etc.—engaged in any particular transaction. Blockchain enables these entities to maintain an official system of record wherein each party can verify they have access to the exact same data, and no party is able to make unauthorized alterations of trade finance records.

Other than financial services, shared data services are the most common and successful application of blockchain technology to date. Shared data services are used for supply chains and logistics, reputation management, asset tracking, real estate and title registry, and much more. For example, the world's largest shipping company Maersk partnered with IBM to use a blockchain application to track goods traveling across its shipping system.[75] Similarly, Dubai, in conjunction with the private sector, has launched a blockchain-based project called the Digital Silk Road to provide transparency within supply chains.[76] These blockchain-based systems allow various entities, such as shipping companies, customs authorities, cargo owners, and freight forwarders, to locate and identify shipping containers anywhere in the world. The tamper-proof record enables trust between all parties because changes are immediately apparent to all, as participating entities can verify the accuracy of information passed along from the entity before it, and can run analytics over the system to prevent counterfeit goods, fraud, and theft. This process improves overall transparency and traceability throughout the system.

Certainly, blockchain will not be the solution to all shared data services. In many cases, blockchain is still in its pilot phase, and the costs of developing and running a blockchain are not yet clear. Moreover, blockchains fall victim to the same challenges that affect other types of databases. For example, blockchain applications are susceptible to garbage in, garbage out issues, wherein flawed input data produces flawed outputs. Indeed, using a blockchain to collect social media data for targeted advertising only works if that advertising can target based on legitimate user interests. To reduce the likelihood of flawed inputs, blockchains can have multiple nodes check and verify the information is correct.

Case Study: Food Contamination

In the past, when there was an outbreak of a food-borne illness, retailers were unable to easily track a given food product back to its originating farms. Today, there is often an extensive investigation by the Food and Drug Administration to find the source. Moreover, large recalls waste food, sink costs for businesses, and harm farmers who get swept up in a large-scale response. Indeed, 2014 data from the U.S. Department of Agriculture found that major food-borne pathogens

cost the U.S. economy roughly $15.6 billion per year.[77]

As a result, companies in the food industry have launched various initiatives to track and trace products from farm to fork. Many supply-chain IT systems use centralized database architectures to tackle this problem, especially those with a relatively small number of known partners and a limited need to independently create consensus around transactions. However, when food supply chains are complex, multitiered, and include many participants that are not necessarily known or trusted, blockchain may be a more efficient way to trace the source of problems in the event of a recall.[78] Some companies have started experimenting with blockchain-based systems to add transparency, trust, and traceability.

Several major food companies have participated in industry-wide food-traceability pilot studies involving blockchain technology over the last few years. The biggest of these studies was done by Walmart.[79] In 2016, Walmart partnered with IBM to use blockchain technology to track mangos through the supply chain—which contained many different retailers, food service organizations, farms, shipping companies, regulators, and more. Individual goods in this complex system can be difficult to track back to any particular farm.

During this pilot, at each stop in the supply chain, people handling food products for Walmart made an entry on the blockchain, noting that they had received the good and passed it along to the next person. After the pilot completed, Walmart was able to use the new system to reduce the time it takes to track the origin of food in its system from a week to a few seconds.[80] The pilot went so well that Walmart sent a letter to suppliers of lettuce, spinach, and other greens to join its food-tracking blockchain by September 2019.[81] Indeed, Walmart claims its blockchain system is better than centralized models because of its diverse set of business partners and the redundant and tamper-resistant nature of the system.[82]

Case Study: Public Records

Public records, including birth certificates, marriage licenses, death records, vehicle registrations, land and deed registrations, and corporate registrations, are those available for everyone to access. Public records databases tend to be centralized within a government agency, requiring citizens to place trust in the government to keep accurate and reliable records. Unfortunately, all too often those records are inaccurate or unreliable, or do not have the proper redundancy in the event of an emergency—particularly in the developing world. For example, in Haiti, an earthquake in 2010 destroyed municipal buildings that held documents proving ownership of land, and as a result, many individuals are still fighting over land to this day.[83] In other cases, the government agency keeping them can be inefficient or even corrupt. In Honduras, for example, government officials have altered ownership databases and stolen property.[84]

Public blockchains enable permanent, time-stamped records of transactions that are auditable to everyone but cannot be changed by any single party. This type of database allows individuals and businesses to access and store their public records and obtain a complete copy of all records. Using blockchain allows the government to publish not just a copy of the official records, but the

official records themselves—and because the official records are on the public blockchain, there is no potential gap between the government's own records and what it makes public. Blockchain can also help with tracking transactions and stopping counterfeiting in public record databases by providing an audit trail. Indeed, because each record in the system is cryptographically linked to prior records, establishing ownership is easy.

Take, for example, a land registry. When a resident wants to purchase property, they generally must register a deed, which requires paper records or scanned images to show ownership in that land has shifted. The problem is some individuals often try to scam the government agencies by submitting forgeries or fake paperwork. This harms legitimate mortgage owners because defects, forged signatures, and bad paperwork can make it more difficult to obtain proper documentation of property ownership.[85]

Blockchain applications enable deeds recording offices to more easily track asset ownership. For example, the Cook County Recorder of Deeds in Illinois ran a successful blockchain pilot for land registry.[86] The pilot found that the blockchain system was "superior to locally isolated client-server models, and can provide a method of recordkeeping that is resistant to alteration, even by government officials."[87] This type of blockchain application is even more useful for the developing world, where there are fewer paper documents that show property ownership, and corruption often allows property officials to change documents (for the right price). For example, the government of Andhra Pradesh in India is using blockchain systems to maintain land records and streamline vehicle registrations as a solution to rampant corruption and a surge of property disputes.[88]

The major challenge with blockchain-based public records systems is the actual digitization of the records. Indeed, for blockchain-based systems to work optimally, all current public records need to be properly authenticated and digitized. Importantly, while digitizing records would lead to massive efficiency gains for users accessing them, those benefits are not unique to blockchain. For example, any public system with digital property records would reduce both the burdens associated with title search and information asymmetry in the title insurance industry. Policymakers will need additional evaluation to determine whether blockchain-based public records systems are better than other digital solutions.

Case Study: Electronic Voting

Many people have called for improvements in election technology to address problems with ballot marking, vote tallying, and election administration. Some people have popularized the idea of using paper audit trails—ensuring a voting machine has a paper receipt.[89] Unfortunately, paper audit trails leave many security holes while introducing new ones, increase the costs of voting, and prevent the use of innovative voting technology that would offer voters more security, transparency, and reliability than paper audits can deliver alone.[90]

Every step of the voting process should be secure. Ballots must be cast as intended, collected as cast, and counted as collected. Paper audit trails only provide verification of the first step—that ballots were cast as intended. While important, it does nothing to prevent election officials from

not counting them—whether by changing tallies or shredding receipts. Voters today must simply hope their ballots are counted and the voting tallies are correct when they see the results on election night.

Improving this antiquated system involves enhancing multiple security controls that verify and count votes throughout the system. It requires software testing for voting machines, physical security, and pre- and post-election audits. Moreover, the system must be accessible and sufficiently user friendly for voters to cast their intended votes in the first place.

To improve the security, usability, and accessibility of voting, all technologies should be on the table, including blockchain. Indeed, the value proposition of blockchain technology lines up with many of these goals. A public blockchain for voting would be a tamper-resistant record everyone could access, audit, check against voter rolls, and use to independently verify the integrity of votes cast. Moreover, blockchain systems allow voting machines to connect to an encrypted network with no single point of failure. For these reasons, some companies have started testing the viability of voting on the blockchain. For example, in November 2018, West Virginia offered a mobile blockchain-enabled voting app for overseas voters to cast absentee ballots.[91] Similarly, the South Korean government announced it would test the use of blockchain technology in its electronic voting system.[92]

Blockchain is not a mature-enough solution to be widely used for electronic voting, but it is reasonable for election officials to pilot the technology and evaluate whether its benefits outweigh the risks.

Smart Contracts

Some applications use blockchain to automate actions or functions. Because blockchains are programmable, developers can encode certain conditions and outcomes so transactions over the network happen automatically. This application is often referred to as a "smart contract," a computer protocol that can facilitate, verify, and enforce the performance of an action or contract on a blockchain. While the concept behind these applications was invented in 1994, most platforms were unable to properly enforce them until they became popularized with the Ethereum platform in 2014.[93]

The ability to automatically enforce complex transaction rules has enabled developers to create innovative decentralized solutions to tackle myriad challenges.

Importantly, "smart contracts" is somewhat of a misnomer. They are simply business rules encoded in software—they are not legally binding without contractual agreements. These

computations can do myriad different tasks, such as managing agreements between users, storing information about an application (e.g., domain registration), and improving existing processes, such as securities trading and trade finance.

The key benefit of smart contracts is they have a disintermediating effect when combined with a blockchain. By creating an agreement between several parties that automatically executes once the terms are reached, there is no need to have a third party execute those terms. As such, smart contract applications greatly improve efficiencies of various applications, such as automating reporting, compliance, and processing; facilitating automatic payment of dividends from securities, derivatives, and other financial instruments; and automatically releasing or destroying data. Indeed, the ability to enforce complex transaction rules has resulted in developers creating many of the blockchain-based decentralized web applications, also called DAPPs, discussed throughout this report.[94]

Case Study: Escrow Services

Escrow services work by placing money in the control of an independent and licensed third party to protect parties making a transaction. For example, if a user wants to buy a piano, the escrow agency can hold the buyer's money and release it once the buyer confirms they have received that piano. An escrow service can also regulate that payment of funds, such as by dolling them out slowly over time. Using this type of financial arrangement comes with compliance costs, such as fees, and limitations, such as restrictions on the amount of money two parties can put into escrow.

Blockchain-based smart contracts completely remove the need for having a third-party escrow service for certain transactions. Smart contracts are their own nodes on the network and can hold funds on behalf of individuals until the programmed conditions occur and the smart contract automatically releases the funds. As a result, smart contracts remove the costly intermediary, cut costs, and generate efficiencies by automating the transaction. For example, the company Propy used a smart contract to replace an Escrow company in a $60,000 land deal.[95]

Decentralized Marketplaces

Many companies are using blockchain to create a peer-to-peer marketplace for the exchange of goods and services. These blockchains reduce intermediary costs to improve efficiencies and allow users to buy and sell with one another directly while establishing a permanent record of the transaction. Moreover, these systems often have payment mechanisms or incentive structures already baked in using cryptocurrencies.

Some decentralized marketplaces are used for general e-commerce, such as the platform OpenBazaar, which allows users to list virtually any good and pay with over 50 types of cryptocurrencies.[96] Other decentralized marketplaces are set up for the exchange of specific types of goods or services. For example, Bounties Network, which functions like TaskRabbit, enables users to advertise and pay for freelance work performed by other users, such as content and design work or translation.[97]

Many of the applications in this category are nascent, and only time will tell whether they will add significant value over existing intermediary-driven marketplaces.

Case Study: Energy Resource Management

Distributed energy resources (DERs) are physical devices, such as batteries, rooftop and community solar, and electric vehicles, characterized by their small capacity and connection to the electric grid. DERs are often behind-the-meter or connected directly to the energy-distribution system. Over the last few years, dropping costs and policies aimed at generating higher levels of renewable energy have led to rapid growth of DERs throughout the world.[98] However, current centralized systems and market structures rely on incumbent utilities to deliver energy by gathering fuel, generating electricity, connecting to the electric grid, and delivering that electricity directly to end consumers. Traditional distribution utility systems are designed for a one-way flow of power to the end consumer and therefore ill-equipped to handle flexible energy output from DERs, which require them to be optimized for two-way power flows. Some types of DERs have significant levels of supply variability, which can result in inefficiencies when operators do not have the proper systems to handle them.[99] Moreover, centralized energy systems are inflexible in user choice and lack the resiliency of decentralized models.

Blockchain-based systems have the opportunity to enable consumers, grid operators, and utilities to use DERs to create a distributed system for managing energy efficiencies and facilitating energy transactions over the grid. Whereas consumers have traditionally been forced to purchase energy directly from utilities, a distributed system of DERs enables them to sell energy directly to one another.[100] As a result, DERs and blockchains have helped enable the rise of microgrids—smaller grid systems linked with localized power sources.[101] This increases consumer choice, as some consumers may want to purchase energy from certain sources, such as those favoring renewables to fossil fuels. These systems also improve grid resiliency over centralized systems that rely on a network of vulnerable poles and wires.[102] In a decentralized system, if a section of poles or wires becomes compromised, users can rely on DERs—such as solar panels, onsite batteries, and generators—not affected by the outage.

When these systems are in place, suppliers and customers will be able to use smart contracts to automate sales by creating parameters that automatically trigger transactions based on the type of energy, price, time of day, location, and more. For example, the European transmission system operator TenneT has partnered with IBM for a pilot program testing whether blockchain can improve the efficiency of DERs.[103] In this pilot, TenneT sends a price signal to participating customers who own electric vehicles or small-scale batteries, can record their availability, and store and sell power back to the grid in order to reduce their own demand, thereby helping make the grid more predictable for TenneT.[104] Another company called Grid+ is rolling out a pilot in Texas that connects devices to a small-scale battery, smart home device, and the home's smart meter to intelligently manage power usage and programmatically buy and sell electricity on behalf of the user.[105]

Case Study: Copyright Monetization

Monetizing copyrighted content can be cumbersome and complex. Take, for example, the music industry. There is a vast ecosystem of entities that both receive and facilitate copyright monetization for music: artists, managers, record companies, producers, rights organizations, distributors, and more. Adding to this complexity are varying royalty rates. Artists often do not get to determine royalty rates for their music, and some rights organizations have to deal with compulsorily licensing the artists they represent.[106] Moreover, businesses that pay for music licenses—such as movies licensing music, terrestrial radio, Internet radio, and interactive services such as Spotify—operate under different rules with different mandated licensing rates.[107] And while the U.S. Congress has started to push some rights organizations into using centralized clearinghouses for certain types of licenses, the landscape for music licensing remains largely offline, disjointed, and complex—especially for those trying to license music internationally.[108]

With a transparent music licensing database that facilitates market-driven pricing, blockchain could usher in a wave of innovation in the digital music world.

In addition, this fragmented system lacks a standard format for music licensing information, and organizations often fail to share it once it has been collected. This has led to different rights databases that have incomplete, incorrect, or mismatched licensing information.[109] To navigate this labyrinthine system, artists often pay a subscription fee to digital distributors, such as the company The Orchard, to publish their music on each platform and then collect licensing fees.[110] Even with these services, artists still do not have an easy way to track the income they should be earning from each of these platforms that enable their music to be streamed.[111]

Blockchain technology offers an opportunity where these centralized database models have largely failed by bringing together disparate databases and parties with conflicting interests to use a unified blockchain for music licensing. This model could remove intermediaries by allowing artists to directly license their music on a blockchain and enable them to receive direct compensation in a streamlined and manageable way. A blockchain-based application could also use smart contracts programmed to navigate the complex legal landscape and operate based on artist- (or court-) defined royalty rates, combined with cryptocurrencies, to automatically pay artists whenever they music is used. Already, major music organizations—including the American Society for Composers, Authors, and Publishers (ASCAP) the Society of Authors, Composers, and Publishers of Music, and Performing Right Society for music—have launched a pilot for a unified industry blockchain for tracking music royalty metadata for performance rights.[112] Moreover, the company RightsLedger, has launched a blockchain-based registration and tracking service for content authentication and content monetization.[113]

This potential application of blockchain is not without its challenges. For example, given that music rights information is often incomplete or incorrect, rights organizations need to better authenticate it before placing it on a blockchain. In addition, more research and development for blockchain consensus mechanisms is also necessary for a single implementation of blockchain to be able to widely help the music industry. Indeed, the streaming services, such as Spotify and Pandora, each handle larger volumes of transactions per second than current blockchains are capable of processing.[114]

Authenticity

Some applications use the distributed ledger and its tokens to create an easily verifiable audit trail to establish the authenticity of goods or data. Tokens can either represent goods or data located directly on the blockchain, such as cryptocurrencies, or real-world assets such as diamonds or tickets. Blockchains secure the provenance and ownership of these tokens through registration and recording events, and changes that impact them—such as an item's value or when it changes hands. The blockchain also prevents counterfeit goods, and deters malicious parties, from manipulating data because nodes in the network can easily notice and reject false changes.

However, there are often challenges with establishing provenance of real-world assets using a blockchain. Indeed, simply registering an item on the blockchain does not prove a physical item is the original, nor does it establish a persistent connection to that item.[115] While blockchain can help with recordkeeping and authenticity, it does not help with appraisal or physical security. Moreover, a fake asset could be registered to a blockchain as a legitimate entry. For example, prior to registering a work of art to a blockchain system, its owner would need to get that art independently authenticated.

Case Study: Combating Counterfeiting and Fraud

Fraud affects most entities across both the public and private sectors. According to the Association of Certified Fraud Examiners, a typical organization loses 5 percent of its revenue to fraud each year.[116] The International Chamber of Commerce estimates pirated and counterfeit goods will sap $4.2 trillion from the global economy and put 5.4 million legitimate jobs at risk by 2022.[117] Fraud is particularly prevalent when there is little infrastructure or government regulation to combat it. For example, due to under-enforcement combined with high demand, worldwide counterfeits for luxury goods alone is estimated to be worth $1.2 trillion.[118] Many companies, governments, and nonprofits are experimenting with blockchain technology to improve the market for goods that have traditionally been rife with fraud, using the relative tamper-proof nature of the blockchain to improve the authentication of goods.

Take, for example, the growing problem of counterfeit drugs.[119] In 2016, the International Trade Administration estimated that revenues from the global counterfeit drug trade were between $75 billion and 200 billion each year.[120] Fake drugs are particularly prevalent in the developing world. Indeed, according to research from the World Health Organization, "An estimated 1 in 10 medical

products circulating in low- and middle-income countries is either substandard or falsified."[121] As a result, the U.S. Congress passed the Drug Supply Chain Security Act of 2013 to require drug companies and their supply-chain partners to more closely track where their finished products are shipped.[122]

Currently, most drug manufacturers use centralized systems to track their supply chains. Unfortunately, these systems are plagued by a lack of transparency, and asset tracking systems that often fail to detect imposter medications. As the Partnership for Safe Medicines explained:

> Counterfeiters can produce look-alike drugs and devices that contain little or no active ingredients, or the wrong ingredients, for less than the authentic medication would cost to make. Criminals duplicate packaging, product shape, taste and feel so that it is indistinguishable from authentic medicine. Patients and doctors can't tell the difference.[123]

Blockchains offer the potential for drug manufacturers to better track drugs in the complex environments that are their supply chains.[124] First, after the drugs are manufactured, workers register them on the blockchain. Next, the system verifies those authentic drugs were only given to authorized parties during transfer points in the supply chain. If a drug disappears or an inauthentic one is added to the supply chain, the system can easily identify its origin. Moreover, workers can use the system to track other variables, such as temperature, to ensure proper conditions are observed during transportation so patients do not receive ineffective medications.

Several companies and nonprofits have launched initiatives to test the potential of blockchain technology to combat this problem. For example, in March 2018, Accenture announced a partnership with logistics company DHL to develop a blockchain-based prototype to trace pharmaceutical products and prevent the shipment of counterfeit drugs.[125] Similarly, Mediledger is an open blockchain project launched in 2017 to help pharmaceutical companies, which join the network as nodes, trace drugs throughout their supply chains and comply with regulations.[126] Moreover, IBM is testing a pilot program in Kenya to better track and authenticate drugs at each stage in their supply chain, from pharmaceutical company to the patient, using mobile technology.[127]

Case Study: Cryptocollectibles

Some companies have started offering users blockchain-based collectibles. Traditional collectibles, like baseball cards and Beanie Babies, were bought for the sake of owning them and appreciated in value with age and scarcity. Some collectors would collect them, allow them to appreciate, and sell them for profit. Before the advent of blockchain technology, digital collectibles were not possible because they were too easy to replicate, making both proof of ownership and scarcity a difficult prospect. However, with blockchain technology, users have a method to prove ownership, and asset creators can create scarcity with unique items.

These blockchain-enabled collectibles, called cryptocollectibles, have grown in popularity.[128] For

example, a company launched a cryptocollectibles game in 2017, called CryptoKitties, wherein users collect non-fungible cartoon cats.[129] Each CryptoKitty has a unique code that gives the cat exclusive attributes. These digital cats are owned by the user, and ownership is validated by the blockchain. The Ethereum blockchain ensures each digital cat is a unique and therefore scarce asset whose value appreciates or depreciates based on the market. In addition to buying and selling these digital cats, users can also essentially "breed" two different digital cats to create unique tradable items. By breeding them, users have the ability to make billions of possibilities. CryptoKitties are popular. Indeed, users have spent more than $25 million buying and breeding digital cats between the game's launch in December 2017 and June 2018.[130]

Digital Identity

A digital identity is information individuals, organizations, or devices use to represent themselves to others in a digital environment. They are composed of data attributes about that individual, organization, or device, such as online authentication information (e.g., screen names and passwords), contact information (e.g., names and email addresses), government identification information (e.g., Social Security and driver's license numbers), device identifiers (e.g., IP and MAC addresses), and financial information (e.g., credit card and bank account numbers). This information is used to facilitate commercial and government transactions, such as taking out a loan or applying for government benefits. Digital identities also allow third parties to authenticate someone is who they claim to be, which is an important function for such industries as the financial services industry, which must abide by rigorous know-your-customer rules designed to prevent money laundering.

Some organizations have adopted blockchain-based applications to establish digital identities or give users the ability to control or obfuscate their identity online. These applications of blockchain strive to improve the efficiency and security of authenticating online identities, especially in cases wherein an application does not rely on third parties, such as the government, to verify an identity.

Most projects in this category are in very nascent stages, suffer from scalability issues, and have not yet proven their value.

Case Study: Identifying Connected Devices

The Internet of Things (IoT) refers to the vast array of physical objects embedded with sensors or actuators and connected to a network.[131] Increasingly, everyday objects are gaining connectivity, from cars to televisions to traffic lights.

One way to secure these devices is to install digital certificates on each one, a complex and costly endeavor. As an alternative, operators can use a blockchain to easily provide a unique identity to each IoT device on a network. The blockchain system also enables devices to securely broadcast messages—called transactions—to one another, and to save permanent records of those messages on the blockchain. Moreover, using smart contracts, an operator of a network of IoT devices can control devices and manage software updates. For example, an operator of a fleet of automated

vehicles using a blockchain-enabled system could use smart contracts to program the cars to automatically get fuel when they are running low or automatically order new parts in the event of a mechanical failure.[132]

Importantly, devices themselves do not need to be nodes on the blockchain. While technically feasible in some cases, it is inefficient. Indeed, operating as a node requires a large amount of computing power and energy from devices that often have limited battery power. Instead, IoT devices can operate on a proof-of-work blockchain as "light nodes," which do not download the complete blockchain but rather only a portion of each block—just enough to validate the authenticity of transactions.[133] Other blockchain-based IoT systems, such as Tangle, use less-resource-intensive consensus mechanisms.[134]

Case Study: Digital Identity Management

Since the invention of the Internet, there has been a shift from users storing sensitive data locally to trusting a third party to store and transmit their personal data. Users may have payment information stored with different websites for convenient online shopping, or share personal information with their friends over social networks. They may lose track of each of the services with access to their data, while intermediaries that store large amounts of personal information are often the target of attacks. For example, the credit bureau Equifax was the target of a major security breach that led to the release of personal information from over 143 million people.[135]

To address this, some organizations are attempting to use blockchain to protect personal information and give users direct control over how their data is used and shared online. The idea is to use blockchain-based identities to replace multiple credentials for purposes of online authentication. These services would give users access to an "identity wallet," which would act as a unique address on the blockchain, much like a digital wallet for cryptocurrencies. This wallet stores digital versions of identifying information and enables users to choose when to share it and whom to share it with.[136] This process reduces the number of entities that need to have access to information, and removes some intermediaries entirely. As a result, this type of system is often referred to as a "self-sovereign identity."

These projects work by using a public key (an address on the blockchain) and an attestation to authenticate personal information, rather than simply storing information directly on the blockchain. An attestation is a claim another entity endorses that is placed on the blockchain and linked to the person. The app creates a one-way hash of the individual's credential, which is signed by the user's key, thereby offering proof the entity provided the data. This works through a cryptographic technique called "zero-knowledge proofs," which allows an individual to prove possession of a credential without revealing it. Any third party requesting that data can look at the blockchain and verify the data is authentic. Notably, these projects still rely on governments or other trusted intermediaries, such as banks, to authenticate attestations before use on a blockchain.

While there has been a lot of hype around developing such a system with blockchain technology,

there are many challenges with this approach. For one, there is a chicken-or-egg challenge. Why would a firm become capable of accepting blockchain-based digital identities when no one else has them, and why would users adopt these identity management systems if they cannot use them anywhere? Unfortunately, many companies pursuing these applications are having problems onboarding users and partners.[137] Civic, one of the largest companies in this space, has only 93 partners—most of which are other blockchain start-ups.[138] For these systems to be adopted, governments and private organizations would have to agree to accept blockchain-based digital identification as valid and work together to create standards for interoperability between different forms of digital identification.

Without a concrete value add from blockchain systems, it is unclear how self-sovereign identity management systems will reach the scale they need to be viable.

Second, it is relatively easy for users to falsify identity information when there is no verification process for information submitted to a blockchain-based identity system. Developers of these systems get around this problem today by scanning and digitizing government IDs.[139]

Finally, and most importantly, many of these processes are easily performed today without the use of a blockchain. For example, companies can scan IDs and offer online verification services.[140] Indeed, a fully digitized identity management system, regardless of whether it used blockchain, would allow users to more easily control access to their information, thereby enabling more efficient e-commerce transactions, facilitating many types of e-government services, and helping to prevent fraud and identity theft by improving the security of online transactions.[141] In addition, other technologies offer benefits not found with blockchains. For example, certain certificate structures, such as X.509, allow companies to verify the authenticity of edits and redactions—something that is difficult to do on a blockchain. Without a concrete value add from blockchain systems, it is unclear how self-sovereign identity management systems will reach the scale needed to be viable.

REGULATING BLOCKCHAIN APPLICATIONS

Because the use of blockchain technology cuts across sectors, from agriculture to finance to human resources, many different regulators have a say in various applications that use blockchain. In the United States, at the federal level, the Department of Agriculture will oversee uses of blockchain in certain food supply chains; the Food and Drug Administration will oversee its use in drug supply chains; SEC will oversee cryptocurrency securities, the Department of Health and Human Services will oversee any blockchain use for health records, the Federal Trade Commission (FTC) will regulate unfair and deceptive practices involving blockchain-based businesses, and many more. And because many of the technology's applications are global in nature, regulators may

create conflicting rules across jurisdictions.

There are several bodies of law that will have immediate policy implications for businesses developing and deploying blockchain technology.

Financial Regulation

There is a lot of uncertainty in how mature financial regulatory systems are approaching blockchain-based applications.

From an international perspective, companies doing business across borders must navigate a complex set of rules to bring their services to global markets, as each country has different financial regulations. Because many blockchain-based financial services are fundamentally international, especially those that function on a public blockchain like Bitcoin, firms face a difficult time scaling their services while also abiding by various national laws. While there are some international efforts to harmonize regulations, most of them center around traditional financial services, such as banks and legacy payment providers.[142]

From a national perspective, each country has its own set of financial laws and regulators, each with varying levels of complexity. In the United States, there are over ten federal regulators for financial services, not including each state's financial regulator and attorney general. Similarly, the European Banking Authority has determined blockchain-based financial assets typically fall outside the scope of EU financial rules, and therefore the European Union needs to craft new regulations for them.[143] Other countries, such as China, have banned certain types of blockchain-based financial applications, such as ICOs, while allowing others to create an environment of high regulatory uncertainty for cryptocurrencies.[144]

One of the primary types of financial regulations that blockchain-based products and services must abide by is anti-money laundering (AML) compliance. In the United States, there are two primary AML laws: the Banking Secrecy Act (BSA) and the U.S. Patriot Act.[145] But there are also several other more-targeted laws, such as the Anti-Drug Abuse Act of 1998 for drug-related money laundering, and the Foreign Corrupt Practices Act of 1977 for illegal actions abroad.[146] As a result of these laws, there are dozens of federal watchdogs that oversee AML compliance. For example, in 2013, the Financial Crimes Enforcement Network (FinCEN)—an agency that operates under the umbrella of the U.S. Department of Treasury—released a paper stating exchanges and administrators of cryptocurrencies are subject to the BSA and must register as a money services business.[147] Indeed, in May 2015, FinCEN took civil action against the virtual currency exchange Ripple Labs for not following AML rules, resulting in a $700,000 fine.[148] Moreover, in 2017, FinCEN issued a letter ordering companies issuing ICOs in exchange for another type of value to abide by "know-your-customer" AML compliance.[149] Many cryptocurrency businesses are struggling to comply with these laws. For example, a 2019 report that analyzed 216

cryptocurrency exchanges found that 69 percent of these businesses failed to have complete and transparent know-your-customer procedures.[150] In addition, these laws are often incompatible with privacy-focused financial blockchain applications, such as privacy coins.

There are also national laws that regulate capital markets, such as how firms offer stocks, bonds, and other investments. In the United States, both the Commodity Futures Trading Commission (CFTC), which regulates commodities futures and swaps trading, and SEC, which regulates securities, have been active in regulating blockchain-based financial applications. Unfortunately, these regulators are often at odds. CFTC classified cryptocurrencies as commodities through a 2015 enforcement action, which is a less-restrictive regulatory framework that enables firms to register with the agency or meet rules for exemption to trade cryptocurrencies.[151] Indeed, CFTC prosecuted the cryptocurrency trading platform Coinflip for offering unregistered bitcoin swaps in 2015.[152]

On the other hand, SEC has issued stricter guidance for blockchain-based assets, particularly ICOs.[153] In March 2018, SEC stated it would apply securities laws comprehensively to everything from digital wallets to exchanges.[154] In April 2019, it released more-detailed guidance about how it determines whether a cryptocurrency or asset is a security, commodity, or other digital asset.[155] In effect, it says SEC will treat all speculative tokens developers use to fund the development of a decentralized platform as securities, while those sold once the platform is working and decentralized are not. While this guidance is not a set regulation, it is bolstered by past SEC enforcement actions and relief. For example, SEC has said cryptocurrencies that are sufficiently decentralized (i.e., the ownership of the cryptocurrency is not concentrated enough in the hands of a few individuals for them to make changes to the system by themselves) are not considered securities.[156] This includes Ethereum and Bitcoin. SEC has also released a letter saying the token offered by TurnKey Jet was not a security because it was not offered with the expectation of profit.[157] SEC has since issued enforcement actions against several entities that issued ICOs for selling securities without a license. For example, in November 2018, SEC brought an enforcement action against Paragon Coin for not registering its ICO.[158] Some companies are challenging the classification of ICOs as securities.[159] Furthermore, SEC has repeatedly denied applications for companies to register ICOs as securities as well as applications to create exchange-traded funds based on certain cryptocurrencies, such as Bitcoin.[160] The Justice Department is coordinating with SEC and CFTC over future cryptocurrency regulations to ensure effective consumer protection and more streamlined regulatory oversight.[161]

Moreover, there are laws that supervise banking and money transmission, involving several regulators. There are many different general federal banking laws, such as the National Bank Act of 1864, the Federal Reserve Act of 1913, and the Dodd-Frank Wall Street Reform and Consumer Protection Act.[162] There are also several federal regulators that oversee these laws, including the Comptroller of the Currency (OCC), the Federal Reserve Board, and the Federal Deposit Insurance Corporation (FDIC). While many of these entities focus on national banks, some have started to focus regulation on other types of financial services.

Subnational governments, such as states, have added to this complex regulatory system by creating their own additional rules and regulations for banks and money senders. For example, because state money transmission laws are based on the location of the customer rather than the business, payment and digital currency businesses must get a state-issued money sender or transmitter license in every state in which they have customers. In some cases, states have passed laws to specifically regulate digital-currency businesses. For example, in June 2015, the New York Department of Financial Services created regulations that were similar to the state's money-transmitter licensing but specific to virtual-currency businesses.[163] Indeed, as of the release of this report, New York has the most comprehensive regulations for digital currencies of any state or federal regulator to date. In contrast, the Colorado legislature passed the Colorado Digital Token Act in March 2019 that exempts the offer or sale of "digital tokens" deployed on blockchain networks from state securities and money-sending registration when certain transactional conditions are met.[164] It is likely other states will add to this regulatory patchwork.

Efforts have been made to reduce this regulatory complexity. For example, OCC has attempted to create a charter for certain financial companies, allowing them to offer deposit and loan services without complying with state regulations.[165] Unfortunately, these rules have been tied up in lawsuits from state regulators.[166] Similarly, several states—Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas, and Washington (collectively, "Signatory States")—have taken steps to standardize licensing practices for payment systems.[167]

BOX 4: MONEY TRANSMISSION LAWS AND THE CUSTODY OF CRYPTOCURRENCIES

Like banks that have custody over the assets in an individual's checking account, which entity has custody of an individual's cryptocurrency matters from a legal perspective because of their ability to act on it—sometimes without the permission of its owner. And yet, cryptocurrency systems can be complex with many different types of entities operating computers that relay information about transactions to maintain the blockchain ledger without actually having custody over any individual's cryptocurrency. Unfortunately, many state money transmission laws have not accounted for which entity has custody of the cryptocurrency, which has led to confusion throughout the industry.[168]

What does custody mean with regard to cryptocurrency? Because cryptocurrency transactions involve at least two distinct keys—a public key and a private key—developers can design blockchain-based services to have access to one of those keys, both, or neither.[169] If a company has their customer's private key, then it has custody over that customer's cryptocurrency and can manage it on their behalf. On the other hand, there are services that simply issue software that allows users to keep the private keys on their home computers, while the company stores their public keys. This type of software wallet does not have custody of its clients' cryptocurrency and cannot make or

receive payments on their behalf. Custody gets more complicated when the public and private keys can be spread over multiple institutions to improve security and key control, as they are with multi-signature wallets.

States have not clearly defined in their money transmission laws what it means to control a digital currency. These statutes often define the terms "money" and "money transmission" very broadly. For example, some statutes apply to any company "controlling" a digital currency without laying out what constitutes "control."[170] As a result, there is a risk of these laws being applied to businesses that do not actually have any custody over customers' cryptocurrency and do not pose any solvency risk to those customers. For example, overly broad laws may accidently affect software wallets or network nodes, neither of which have custody over cryptocurrency. In contrast, companies such as Coinbase not only offer secure storage, but also utilize their custody over cryptocurrencies in order to provide interest payments.[171]

Some lawmakers have attempted to remedy outdated state money transmission laws. In 2018, Rep. Tom Emmer (R-MN) introduced the Blockchain Regulatory Certainty Act, which would create a safe harbor from state money-sending laws for blockchain developers and providers of blockchain services that do not have custody of digital currency.[172]

Finally, other regulators in the United States have also started assessing blockchain-based financial applications. For example, the Financial Stability Oversight Council, which comprises the heads of all major federal financial regulators, including the Secretary of the Treasury, Federal Reserve Board of Governors, and the chairmen of SEC and CFTC, assesses financial system risks, has formed a group on cryptocurrencies.[173]

Consumer Protection

There are multiple federal and state regulators governing legal prohibitions on unfair, deceptive, or abusive practices for blockchain-based applications. Some of them are general enforcement agencies, such as the FTC through its unfair and deceptive practices authority.[174] Others are focused on a narrow industry, such as the Consumer Financial Protection Bureau (CFPB) for financial services and FDIC for banks. At the state level, several laws give state attorneys general the ability to sue businesses for unfair and deceptive or abusive practices.[175]

As the major regulator for consumer protection, the FTC has used its authority to bring enforcement actions against a wide range of entities who have not kept the promises they have made to consumers in their stated policies. The FTC does not have authority over certain industries and entities, such as banks, savings and loan institutions, and common carriers, which are regulated by other federal agencies, nor does it have regulatory authority under the Administrative Procedure Act. When a company acts unfairly or deceptively, the FTC can bring enforcement

actions that result in a consent decree, whereby the company faces penalties for future misconduct. During the span of a consent decree—which can last up to 20 years—the FTC may subject a company to audits, the results of which could be violations with significant fines.[176] In addition, the FTC has conducted several conferences on various technologies and sectors, including financial services technologies, to better understand enforcement in this space.[177]

CFPB has already been issued several actions related to cryptocurrencies. In 2014, the bureau released an advisory that warned consumers of the dangers of cryptocurrencies and started accepting related consumer complaints.[178] CFPB has also brought related enforcement actions. For example, in March 2016, CFPB imposed its first consent decree with a $100,000 penalty on Dwolla Inc.—an Iowa-based peer-to-peer payment system—for misrepresenting its data security practices by failing to implement appropriate security measures.[179]

In addition to prohibitions on unfair, deceptive, and abusive practices, financial disclosures are often the centerpiece of consumer financial protections. As a result, there are a number of federal laws that require disclosures, such as the Community Reinvestment Act, the Equal Credit Opportunity Act, the Fair Credit Report Act, the Fair Debt Collection Practices Act, the Fair Housing Act, the Real Estate Procedures Act, the Truth in Lending Act, the Trust in Savings Act, and securities laws all require financial institutions to provide detailed disclosures to consumers.[180]

Privacy

Regulations that affect how organizations can collect, use, and share data can affect blockchain deployment. The European Union's General Data Protection Regulation (GDPR), for example, grants several rights to European citizens while restricting how organizations handle data.[181] One of its provisions effectively prevents the use of many blockchain applications by mandating organizations delete personal data on request, something that is difficult for a tamper-resistant ledger to do. Other countries can restrict blockchain deployment by restricting data-sharing outside their national borders.

In the United States, there is no single federal data privacy law for the private sector. Instead, there are multiple privacy laws and regulators. Some laws create privacy rules for a specific sector, such as health care or financial services, whereas others focus on providing specific safeguards, such as protecting children's privacy.[182] Certainly, many different organizations are pushing to update the U.S. code with additional federal privacy rules—although these efforts have so far not succeeded.[183] On a subnational level, different states have additional protections for certain types of data. For example, California has additional data protection rules for health and financial information.[184] As of spring 2019, there are ongoing discussions about enacting a general federal privacy law in Congress.[185] It is possible such a federal privacy law could have substantial consequences for blockchain deployment.

Digital Content Regulation

Governments frequently create rules that prohibit the publishing or sharing of certain types of information, such as hate speech, libel, and more.[186] Some laws are targeted toward certain behavior or actions specific countries believe are bad. For example, France and Germany have laws prohibiting anti-Semitism and other forms of hate speech, Spain and the Netherlands have lèse-majesté laws that prohibit insulting the monarchs, and some Middle Eastern countries have laws prohibiting apostacy (i.e., the renunciation of religion) and blasphemy.[187] Other laws prohibit content that is generally considered criminal, such as child pornography. Moreover, most countries have intellectual property laws that restrict the use of content protected by copyright, patents, or trademarks without permission or compensation.

Countries often target illicit information by regulating intermediaries. For example, roughly 25 countries have enacted policies that require Internet service providers to block websites that engage in widespread copyright infringement.[188] Others, including the United States, have created notice-and-takedown regimes that grant online intermediaries liability protection for the content posted by users, as long as they remove known infringing content immediately after it comes to their attention.[189]

Because public blockchains are peer-to-peer networks, without intermediaries, that enable the sharing of information in a way that is very difficult to amend, edit, or retroactively change, there is a risk that some users could abuse the technology to store prohibited content in a manner that is difficult to remove. Once placed on a blockchain, any individual that downloads the ledger would theoretically have immediate access to that prohibited content. For example, one report found a graphic image of child pornography within the Bitcoin blockchain.[190]

Fortunately, current versions of public blockchains are not optimal solutions to storing or sharing illicit or pirated content. First, storage capacity on most types of blockchain applications is limited. For example, the storage capacity of a Bitcoin block is only 1 megabyte, although soft forks have enabled some nodes to create slightly larger ones.[191] To store illegal content on most public blockchains, criminals must often bury links to it alongside transaction data, rather than store it in the form of image or video files. Second, inserting data on some public blockchains, let alone locating and decoding it, requires a large amount of effort.[192] Third, public blockchains are pseudonymous records of information uploaded by individuals. Therefore, similar to terrorism financing, cybercrime, and money laundering, it is possible for law enforcement to use the public record to identify criminals.

Taxation

Taxation of blockchain-based assets differs widely between countries. For example, in Israel, cryptocurrencies are taxed as an asset, while Spain subjects cryptocurrency holders to income tax.[193] In the United States, the Internal Revenue System (IRS) treats cryptocurrencies as commodities for tax purposes, including for capital gains. href="#_edn194">[194]

There are several unresolved issues regarding the taxation of cryptocurrencies in the United States. For example, while the IRS treats cryptocurrency as a commodity, the agency does not have a de minimis exemption for cryptocurrencies. Therefore, each time an individual uses a cryptocurrency to make a transaction, such as to purchase a good or service, if its value increased before the transaction then it is theoretically subject to capital gains taxes.[195] As a result, every time anyone uses cryptocurrency to purchase anything—even if the transaction is worth a few pennies—they are obligated to report it on their taxes. In contrast, owners of foreign fiat currency enjoy a de minimis exemption, so if they experience a small gain due to exchange rate fluctuations as the result of using a foreign fiat currency to make a purchase (i.e., buying something abroad worth less than $200), they are not required to report that transaction on their taxes.[196] To address this issue, Rep. David Schweikert (R-AZ) and former Rep. Jared Polis (D-CO) introduced the Cryptocurrency Tax Fairness Act in 2017, which would create a tax exemption for de minimis capital gains—transactions under $600—from personal cryptocurrency transactions.[197]

Gambling

Some blockchain-based applications have created prediction markets, which subject them to gambling laws. Countries take different approaches to regulating online gambling. For example, the United Kingdom Gambling Commission requires licensing, while Australia allows only certain types of gambling services, such as sports betting.[198] In the United States, prediction markets for certain types of betting are legal, while others are not. The Federal Wire Act prohibits bets and wagers on sports events or contest and the Unlawful Internet Gambling Enforcement Act (UIGEA) of 2006 prohibits banks and other financial institutions to process transitions between U.S. residents and gambling sites.[199] In addition, the Illegal Gambling Business Act may also prohibit offshore betting on blockchain-based gambling sites.[200] Moreover, some forms of betting, such as wagers on the future price of a commodity or asset, called binary options, are regulated by CFTC.[201]

Even though online gambling is largely not permitted, some blockchain platforms are testing these rules. Augur, an Ethereum-based prediction market, uses smart contracts to allow users to make wagers on everything from election forecasts to increases in the price of gold to celebrity deaths.[202] These smart contracts automatically collect bets and distribute winnings without identifying participants. However, due to the distributed nature of Augur's protocol, the developers claim they cannot choose what users do with the system and do not have the ability to halt bets.[203] Similar to peer-to-peer file-sharing networks, such as Napster, which facilitated online piracy, betting markets with no intermediaries will have significant implications for law enforcement. With anonymous peer-to-peer gambling over these networks, enforcement may need to be directed at the individual rather than the intermediary. Current regulators, such as CFTC, are not set up to enforce this.

Antitrust

Competition is alive and well among various types of blockchain platforms. In the public

blockchain space, platforms compete for nodes, users, and apps, while individual applications compete with one another for users, investors, and participants. Bitcoin has roughly 50 percent of market share for all cryptocurrencies, with Ethereum following at 10 percent and XRP at 9 percent.[204] Private blockchains also compete to offer services to prospective clients. Moreover, blockchain-based business models are competing with traditional business models, especially as they reduce costs and eliminate intermediaries.[205]

However, blockchain-based applications are not immune to antitrust concerns, such as exclusive dealing, predatory pricing, and other exclusionary abuses.[206] This is especially the case when a consortium of entities can choose to include or exclude other members from a blockchain. Standards setting can also elicit antitrust concerns. For example, established standards setting a consensus protocol that favors certain network members over others could be subject to review. Moreover, if nodes on a network gain over 50 percent of computer power in the network, they can steal from other users on the network and set anticompetitive transaction costs. This increase in concentration may one day lead to oversight, either by mining operations themselves or by government to protect against anticompetitive conduct.

General antitrust enforcement is primarily the domain of the U.S. Department of Justice (DOJ) and FTC. However, certain federal regulators and agencies have oversight regarding consolidation in particular sectors (e.g., the Federal Communication Commission oversees certain media consolidations). Sometimes these regulators work in partnership. For example, DOJ reviews mergers of banks with the assistance of the Federal Reserve.

PRINCIPLES TO ADVANCE BLOCKCHAIN

Given the potential of blockchain technology to improve the efficiency and effectiveness of certain processes, policy should tilt toward enabling organizations to experiment with it. The following are 10 principles policymakers should follow as they assess how and when to support and regulate blockchain applications.

1. Ensure Tech Neutrality

Policymakers should adopt technology-neutral rules that neither favor nor disadvantage any particular application or business model in order to create a level playing field for innovation.

Policymakers should strongly support efforts to increase digitization, but be neutral as to what technology is best suited for any particular application.

Policymakers adopting technologies should ensure they take a tech-neutral approach to different applications. Digitizing processes, for example, offers benefits irrespective of the technology being

used. Instead, policymakers should look to the unique benefits of a technology and the particular challenges of a project when deciding what technology to adopt. Some projects will require traditional centralized approaches for efficiency, while others may be better suited for distributed, tamper-resistance blockchains. For example, a digitization project that requires many different entities to provide inputs, without any particular entity controlling those inputs, may call for a blockchain.

In addition, regulators should apply the same rules to different technologies used to offer similar products and services. Regulators do not necessarily need regulations simply because blockchain applications are different. When confronting a new technology or business model, regulators should first look to existing rules to see whether they apply to emerging applications, which would create a level playing field between the traditional and emerging technology or business model. Clearly, all technology applications are not the same. The concerns associated with money-laundering abuse from unregulated digital currencies may not be the same as from centralized-database-driven traditional banking. Wherever there are differences in technologies, policymakers should establish rules that recognize the risks that are distinct—or irrelevant—to particular applications.

Unfortunately, some regulators have failed to act in a tech-neutral way when it comes to blockchain-based applications. For example, virtual-currency businesses often function similarly to mobile-payment businesses and international-transfer services. However, when New York drafted its Virtual Currency License, called BitLicense, it subjected virtual-currency businesses to different requirements than similarly situated money senders, such as by requiring more arduous anti-money laundering reporting requirements.[207] Policymakers should avoid arbitrary distinctions such as this.

2. Actively Support Blockchain Adoption and Deployment

Policymakers should actively support government adoption and deployment of blockchain, primarily in two ways.

One way is by adopting blockchain applications for their own services. By becoming early adopters, national, subnational, and local governments can promote broader adoption of blockchain. This would also help reduce risks associated with blockchain applications and encourage others to adopt and invest in the technology. These efforts should also include adopting solutions from blockchain companies to improve government operational-reporting, transactions, asset-tracking, supply-chain, management, procurement, and budgetary decisions. For example, the U.S. Department of Health and Human Services recently deployed a blockchain tool to help it buy services and modernize its cloud capabilities, saving money in the process.[208]

To accomplish this, governments may need to reform their procurement processes. Indeed, the U.S. federal government has outdated and burdensome rules and practices governing how federal agencies may purchase technologies. For example, there are a few methods by which the government can make procurements, including contracts—such as the General Services Administration (GSA) Multiple Award Schedule contracts—and open-market acquisitions.[209] Using

these contracts, federal agencies establish Blanket Purchase Agreements (BPAs) with contractors to fill ongoing needs for supplies and services. Unless federal IT vendors are able to establish a blockchain solution on an existing BPA, federal procurers are restricted from buying it—except through open-market acquisition.[210] Open-market acquisition allows agencies to purchase commercial products and services not already under any federal contract. However, open-market acquisition is a slower process that is subject to additional determinations—such as whether a purchase is "fair and reasonable"—before agencies can purchase new goods or services.[211] Furthermore, because it can take six months to a year to update BPAs, by the time the procurement process has resulted in the purchase of a particular product, the next generation of that product has typically already hit the market. This is especially true with rapidly developing technologies, such as blockchain. To reform this process, GSA should establish a blockchain service acquisition unit tasked with facilitating agency procurement of blockchain technology. By developing a core team of government procurement experts for blockchain at GSA, who can advise and facilitate blockchain-related procurement at other agencies, the federal government can ensure it effectively uses blockchain and avoids wasting money on projects that are not viable candidates for the technology.

Second, agencies should reform their internal processes to be able to gather information, better educate themselves, and work directly with companies offering nascent products or services. Many companies are starting to use technologies such as blockchain for regulatory compliance, often referred to as regtech.[212] These solutions not only allow businesses to better comply with regulations, they also improve the quality and efficiency of supervision by giving regulators access to modern reporting and analytics infrastructure they can use to find and correct misuse. For example, CFTC has recommended adopting blockchain technology for swaps markets, hoping it will allow for near-real-time oversight.[213]

In many cases, policymakers will need to authorize agencies to participate in these projects, enabling them to coordinate with companies to better understand them. For example, under its statute, the CFTC is prevented from participating in innovative fintech projects without first having to pay for them.[214] As a result, CFTC needs a legal method of either quickly sharing information between the agency, the businesses introducing new technology, and business models or participating in proof-of-concept blockchain applications. To address this issue, Rep. Scott Austin (R-GA) introduced the CFTC Research and Development Modernization Act in 2018 to give CFTC additional flexibility and authority.[215] When coordinating with firms, regulators should ensure these processes do not favor individual firms or types of technology, cause substantial harm to consumers, or operate in a way that increases systemic risk.

3. Support Blockchain Research and Development

Government investment in research and development (R&D) has played a key role in developing various other technologies, such as smartphones and the Internet.[216] Because early-phase technology research often proves concepts rather than creates commercially viable products, and can exhibit significant spillovers, firms are likely to underinvest. Therefore, national governments should fund R&D for blockchain applications, focusing on underlying technological challenges,

such as creating better and more efficient consensus mechanisms, identifying security threats, improving cryptography, scalability, editability, and more. R&D can also help advance related technologies that could improve blockchain applications, such as quantum computing. Moreover, certain problems, such as intellectual property control management over public blockchains, will require additional research and cooperation from the public and private sectors to ensure enforcement.

4. Promote Legal Certainty for Blockchain Applications

For everyday users to place trust in blockchains, they must be confident the information can be used in legal disputes. As this report has shown, blockchains offer the potential to record, secure, and share a ledger of transactions in perpetuity. As a result, entities in both the public and private sectors have embraced the technology. However, whether blockchain transactions and user signatures on blockchain-based accounts are legally binding is not settled law.

In the late-1990s and early 2000s, users were rapidly starting to use the Internet for commerce. But while U.S. laws gave legal legitimacy to "wet" signatures, they did not do the same for digital ones. To remedy this, U.S. states adopted the Uniform Electronic Transactions Act (UETA) in 1999, which set requirements for electronic signatures to be valid.[217] UETA allowed electronic records or signatures to satisfy states' signature requirements as long as all parties to the transaction agreed to proceed electronically. However, only 47 states adopted UETA. To create a universal framework in the United States, in 2000, Congress passed the Electronic Signatures in Global and National Commerce (ESIGN) Act, which enforced provisions of the UETA in all states.[218] The ESIGN Act effectively preempts states from creating additional e-signature laws unless they follow the original version of UETA, or specify "alternative procedures or requirements that are consistent with ESIGN, do not give greater legal status to a specific technology within the parameters of ESIGN, and reference ESIGN if enacted after its adoption."[219]

However, the legal status of electronic signatures on the blockchain was not laid out in ESIGN or UETA. To give this new technology legal certainty, a few states have passed laws legitimizing blockchain-secured records and signatures under their version of UETA.[220] For example, Delaware and Arizona have passed these laws.[221] However, ESIGN may preempt states from giving blockchain technology legal legitimacy.[222]

Just as when signatures went from wet to digital, there is currently a need for standardized law that gives all forms of signatures legal legitimacy. In the short term, Congress should pass a resolution affirming its intention with ESIGN was not to preempt states from giving legal certainty to new technologies. However, Congress should go further and create an amendment to ESIGN that establishes all blockchain-secured records and smart contracts as legal e-signatures.

5. Rules for Blockchain Applications Should Ultimately Be National, Not Subnational

One of the largest challenges of regulating Internet-based business models is they are often subject to the jurisdiction of subnational governments, such as states, that create their own rules and regulations. When compounded, a company offering blockchain-based solutions across the United States could face rules from each state and territory where it operates, not including federal requirements. This system creates unnecessary and unreasonable compliance costs on businesses and threatens the viability of a national market. This issue is especially problematic for blockchain-based payment companies, which must comply with robust state-based compliance regimes.[223]

A better approach would be for all states to either defer to the national government or work in partnership to create a single, national approach to policy. In the former situation, U.S. states would give the federal government a grace period wherein Congress or federal regulators would have the right of first refusal for creating rules that govern a particular blockchain-enabled service.

Wherever regulations do not exist and regulators think they are needed, national policymakers should strive to create them. For example, both CFTC and SEC have claimed they do not have enough legislative authority to regulate cryptocurrency exchanges.[224] As a result of this vacuum, state regulators have moved to create rules for exchanges.[225] National policymakers should give federal regulators the authority they need to create a nationwide framework for cryptocurrency exchanges.

If national regulators choose not to regulate a blockchain application, and subnational governments, such as state regulators, still believe they need to intervene, they should do so. And subnational governments should cooperate to harmonize their policies and prevent undue burden on companies operating across borders. For example, seven states are attempting to standardize licensing practices for payment systems.[226]

6. Create a Flexible Regulatory Framework That Enables Experimentation

For certain bodies of law, such as financial regulation, the United States has a mature regulatory environment, wherein emerging innovative products and services are often halted by regulators because they do not fit neatly into predefined categories within the law. This is especially true for decentralized applications. In addition, state and federal regulators often butt heads over who has what authority to regulate emerging applications. Blockchain-based services caught in the regulatory tug-of-war are often unable to launch in the United States due to the uncertainty whether their products could draw enforcement action from these regulators. For example, in December 2018, the stablecoin project Basis announced it would stop operating and return the $133 million it had raised in capital because the developers' project was in conflict with transfer restrictions required by rigid SEC regulations.[227] Similarly, the blockchain-based application Sweetbridge launched its supply-chain-finance product in Arizona, rather than nationally in the United States, because it was able to get special permission for a limited trial in that state, while federal regulators would not approve it.[228]

To address this problem, agencies should adopt administrative processes to enable experimentation. They should primarily do so in three ways.

First, regulators need administrative processes in order to understand and categorize blockchain-based products and services. Determining, for example, whether regulators should approach a blockchain-based commoditized token sale used to monetize copyrighted works that was issued in an IPO invokes intellectual property law, securities law, commodities trading law, and more. Indeed, crypto-assets can differentiate based on the technology, transaction speed, utility, decentralization, and many other factors. To better understand crypto-assets, regulators should set up specific committees or working groups that work to understand and classify emerging products and services. For example, in January 2018, CFTC's Technical Advisory Committee recommended the agency adopt a virtual currency subcommittee whose job would be to help the agency differentiate between different types of assets and better understand how to regulate them.[229] Efforts such as these should rely on interagency communication and coordination to ensure agencies do not create conflicting classifications.

By creating flexible and permissive ways to regulate, agencies can send signals to the market about what behaviors are permissible without having to resort to expensive and time-consuming enforcement actions.

Second, regulators can create alternative administrative tools to provide relief to companies, without having to resort to enforcement actions. Regulators can do this through no-action letters, which are applications submitted, along with data-sharing agreements, to the agency about a certain product or service. If the agency accepts the application, it agrees not to bring action against the product or service. No-action letters allow regulators to send a signal to the market about what behaviors are permissible, while allowing financial services to innovate around those signals.

Moreover, regulators can create regulatory sandboxes that give a product or service a safe harbor, with no-enforcement-action relief that enables them to test the product or service in a confined environment under the watchful eye of the regulator. In a regulatory sandbox, the company signs up for a data-sharing agreement, thereby enabling the regulator to work hand-in-hand with industry to allow for more innovative solutions to come to market. To mitigate any dangers that could result from a sandbox, regulators have the ability to revoke these safe harbor agreements in the event the recipient has demonstrated failure to comply in good faith with the terms and conditions, or the company has caused material, tangible harm to its consumers. Importantly, this administrative process should not be blockchain specific. It should enable innovators of all kinds to bring new products and services to market in complex regulatory environments, thereby facilitating competition.

Sandboxes are becoming increasingly popular around the world. The United Kingdom's Financial

Conduct Authority launching its regulatory sandbox in 2016 has enabled 29 firms to test their financial applications.[230] In Singapore, the 2016 sandbox experiment has so successful, the financial authority launched a second iteration with fast-track approval.[231] In the United States, Arizona has launched its own regulatory sandbox effort.[232] Moreover, CFPB has initiated a rulemaking process to create a product sandbox and improve its no-action letter policy.[233]

Third, regulators should enable industry self-regulation. Self-regulation is a vital part of the digital economy, allowing a host of diverse industries to govern industry practices in a range of issues.[234] Businesses use self-regulation to decrease risks to consumers, increase public trust, and combat negative public perceptions. Where standard regulations may be rigid, self-regulation benefits the economy by creating a more flexible regulatory environment than is typically found with government regulation. Industry experts review current activities, identify best practices, and develop them into industry guidelines. These processes can also eliminate conflicts of interest, jurisdictional conflicts, and legal limitations.[235] Ideally, self-regulation would include all stakeholders, produce clear and transparent rules, and be overseen by an independent organization to assess its effectiveness.

For blockchain-based applications, self-regulatory efforts are already underway. For example, several cryptocurrency exchanges together created the Virtual Commodity Association, a self-regulatory organization (SRO) to oversee the burgeoning U.S. crypto trading market.[236] Moreover, the Japan Virtual Currency Exchange Association, an SRO established in 2014, is authorized to develop regulations and oversee registration for the cryptocurrency trading services in Japan.[237]

Of course, self-regulatory efforts are not without government oversight. These self-regulatory frameworks often work best when augmented by baseline levels of regulation and backed up with regulatory enforcement. For example, through its "unfair or deceptive acts" enforcement, the FTC brings enforcement actions against any entity that has not kept the promises it made to consumers in its stated privacy or cybersecurity policies. These enforcement actions can result in a consent decree, whereby the company faces penalties for future misconduct. During the span of a consent decree—which can last up to 20 years—the company may be subject to an audit by the FTC, and violations can result in steep fines. While this type of enforcement is imperfect and can be a backdoor to de facto regulations, it allows for regulators to police voluntary self-regulatory principles.[238]

7. Use Targeted Regulatory Enforcement to Incentivize Companies to Protect Consumers

To maximize the effectiveness and minimize negative effects of enforcement action, regulators should create a system of incentives that promote desirable behavior and discourage undesirable behavior in a marketplace, doing so in a way that limits compliance costs. However, regulators can also go too far and regulate against companies acting in good faith to bring an innovation to market. This approach would limit innovation involving new technologies, such as blockchain (but not limited to it), because if innovators fear they will be punished for every mistake, no matter how

innocuous, they will be much less assertive in trying to develop the next blockchain application, and will spend more time and effort on compliance rather than innovation. For example, penalizing a company for a small technical violation of its privacy policy that caused little or no harm to consumers will likely push that company to spend more resources on lawyers rather than on improving the product itself.[239]

Instead, regulators should evaluate enforcement actions based on two dimensions: whether the company acted intentionally or negligently, and whether a company's action resulted in real consumer harm.[240] Regulators would then use a sliding scale to determine penalties, wherein unintentional, harmless actions receive no penalty while intentional, harmful actions receive large penalties. As they evaluate enforcement actions, regulators should treat negligence as intentional. This strategy would not punish companies for innovating and would instead send them clear signals about what behavior are considered off-limits to better protect consumers.

8. Avoid Laws and Regulations That Effectively Prevent the Use of Blockchains

Policymakers should avoid laws and regulations that would effectively prevent the use of blockchain technology.

This type of inadvertent ban primarily occurs with three types of policies. First, policies that weaken encryption standards can effectively prevent businesses from using blockchain technologies because these technologies rely on strong cryptography to function. Governments around the world have both activity and surreptitiously attempted to weaken encryption, such as by working to weaken encryption standards or requiring extraordinary access.[241] These policies have knock-on effects on the use of several types of technologies, such as blockchain, cloud computing, and mobile telephony.

The drafters of the European Union's GDPR failed to contemplate the law's effects on emerging technologies.

Second, some forms of regulation have mandated that organizations have the capacity to obfuscate or delete certain types of data. For example, the GDPR gives Europeans the right to request businesses delete their personal data under certain circumstances.[242] Similarly, the Stop Enabling Sex Traffickers Act also holds sites liable for knowingly assisting, facilitating, or supporting third parties engaging in sex trafficking.[243] The first problem with certain blockchains, especially public ones, is there is no central entity to regulate them. Whereas in the past there was an online intermediary, such as a website operator, that a judge could demand take down the unwanted information, with public blockchains, many different nodes hold identical copies of the information, so there is no way for any node to edit the blockchain unless all agree to do so.

Certainty, some public blockchains, such as Ethereum, have the capacity to use smart contracts to obscure data stored on the public blockchain, removing the ability for users to access it.[244] However, this information is not deleted, per se.

Mandated data removal from a blockchain becomes difficult when dealing with certain types of enforcement protected by national law, treaties, or trade agreements. For example, intellectual property protection laws, such as the Digital Millennium Copyright Act and the United States-Mexico-Canada Agreement, allow rights holders to request companies take down certain infringing materials.[245] Fortunately, intellectual property theft is a de minimis activity on current blockchain networks. If this trend changes, like-minded nations should work together to ensure enforcement of these protections, be it through enforcement against individuals or blocking of pirated content.

Third, data localization requirements that confine data to within a country's borders can preclude the use of a blockchain system for that data. By restricting the flow of certain types of data, these countries effectively prohibit the use of global blockchains wherever network nodes may exist in many countries. Data localization can be explicitly required by law or be the de facto result of a culmination of other restrictive policies that make it unfeasible to transfer data, such as requiring companies to process or store a copy of the data locally, or mandating individual or government consent for data transfers.[246] Countries justify these policies primarily using three rationales: privacy, security, and enabling government access to data.[247] Other restrictions, such as the GDPR's prohibitions on international transfer of data, do not embrace data localization per se, but rather default to preventing data transfers unless other countries have appropriate safeguards for personal data.[248] These prohibitions effectively prohibit the international use of blockchain-based applications because every node in the system would have access to the same data. For example, if their country adopted rules forbidding the transfer of their personal financial information abroad, these rules would affectively prohibit using a global cryptocurrency.

9. Promote Data Interoperability for Blockchain Applications

National and supranational governments (e.g., European Commission) should also promote data interoperability—the ability of different IT systems to communicate, exchange data, and cooperatively use that data—especially between different types of blockchain technologies, traditional industry frameworks, and regulators. This interoperability may depend on the industry sector and the degree of data standardization therein. For example, streamlining interoperability in datasets for importing and exporting food can help reduce costs for businesses, and help regulators easily share that information across borders. Though industry should lead standards development, national governments can bring together disparate market players across different industry sectors and standards bodies, and encourage and promote interoperability across different types of data.

10. Work to Establish International Harmonization of Blockchain Regulations Across Sectors

Blockchain applications, especially public blockchains, often function more similarly to the broader Internet than technology usage by individual companies. Global systems such as these present unique challenges for policymakers in all nations. Countries will inevitably create their own regulations regarding blockchain-based applications, and many will conflict. This can create a complex framework for businesses operating in multiple countries, let alone a public blockchain that can be downloaded by anyone.

ITIF developed aframework for global policymaking to tackle these types of challenges, lessons from which should be applied to blockchain technologies.[249] First, if the issue involves a multinational blockchain's technical architecture, then countries should rely on and work within an existing global, multi-stakeholder entity to change core functions. Second, if an issue directly affects individuals or companies outside the country's borders, then countries should look to formal international agreements on the subject. If there is a conflict, then the policy should not be pursued. If the policy does not conflict with international agreements, then the final question is whether an informal consensus exists among countries that a certain policy goal is desirable. If this consensus exists, countries can pursue that policy, cautiously ensuring they minimize its impact on individuals outside their borders. These countries can then work to build a formal international consensus on the policy. If there is no consensus, countries should work to build that consensus or find a policy alternative that does not affect people outside their jurisdiction.

The goal of this process should be to align rules and regulations across borders, particularly for public blockchains. Unlike the Internet, however, different global applications of blockchain will be sector-specific in nature, and regulations should reflect this trend. There will be global blockchains for financial services, trade, health care, and many other applications. Rather than create a new international body for regulating blockchains— such as the International Telecommunications Union for communications technologies—these efforts should be developed from existing international efforts in particular domains.

Take, for example, financial services. Beyond individual implementations of behind-the-border rules, governments should seek to harmonize their laws and regulations that focus on the financial services industry and could impact blockchain use in this sector, such as rules affecting routing transactions, transparency, anti-money-laundering, regulatory compliance, and international access to financial data for law enforcement. For example, the International Organization of Securities Commissions (IOSCO) is an ideal forum for harmonizing issues related to securities and futures markets.[250] A sound international framework of cooperation and coordination based on harmonization is essential to effectively regulating and supervising blockchain applications, reducing systemic risks to financial stability, and ensuring innovation in financial services proceeds apace. Governments should also avoid restricting financial data flows and actively push back on localized barriers to them.

CONCLUSION

The applications of blockchain technology have elicited excitement that has resulted in a diverse and interesting set of test cases that attempt to determine when a decentralized application is

better than its centralized counterpart. While some of the case studies discussed in this report may ultimately fail, many will succeed in showing blockchain's strength in eliminating trusted intermediaries while maintaining trust in an official system of record. Only time will tell what the next "killer app" for the blockchain will be.

Policymakers can help this future come to fruition by actively supporting the development and deployment of the technology, when it makes sense—both through adopting it into their own processes and supporting research into decentralized applications. Policymakers should ensure rules for blockchain applications are technology neutral and strive to reduce compliance costs by establishing harmonized regulations, either nationally or, as in the case of regions like Europe, at the European Commission level. Regulators should support innovation by adding flexibility into their regulatory frameworks to enable experimentation while pursuing regulatory actions against companies based on established tangible harms, such as fraud. They should avoid burdensome rules that effectively prohibit the use of distributed ledgers and cryptocurrencies. Most importantly, policymakers should strive to protect and support innovation in blockchain systems.

ENDNOTES

1] Satoshi Nakamoto, "Bitcoin: A peer-to-Peer Electronic Cash System" (Bitcoin.org, October 2008), accessed February 25, 2019, https://bitcoin.org/bitcoin.pdf.

2] Samburaj Das, "R3 Blockchain Consortium Adds 12 More Banks; Will Soon Integrate Financial Services Firms," *CCN*, December 17, 2015, accessed February 25, 2019, https://www.ccn.com/r3-blockchain-consortium-adds-12-more-banks-will-soon-integrate-financial-services-firms.

3] Sarah Buhr, "Long Island Ice Tea Shares Went Gangbusters After Changing its Name to Long Blockchain," *TechCrunch*, January 2018, accessed October 22, 2018, https://techcrunch.com/2017/12/21/long-island-iced-tea-shares-went-gangbusters-after-changing-its-name-to-long-blockchain/.

4] "SEC Charges Digital Asset Hedge Fund Manager With Misrepresentations and Registration Failures," U.S. Securities and Exchange Commission, press release, September 11, 2018, accessed February 25, 2019,https://www.sec.gov/news/press-release/2018-186.

5] "Trade Tech – A new Age for Trade and Supply Chain Finance" (World Economic Forum and Bain & Company, 2018), accessed January 4, 2018, https://www.weforum.org/whitepapers/trade-tech-a-new-age-for-trade-and-supply-chain-finance.

6] Karan Kwatra, "Blockchain: The Byzantine Generals Problem," *Medium*, November 22, 2017, accessed February 25, 2019, https://medium.com/wolverineblockchain/blockchain-the-byzantine-generals-problem-2f17097bad73.

7] Turner Schumann, "Consensus Mechanisms Explained: POW vs. POS," *Hackernoon*, April 5, 2018, accessed February 25, 2019, https://hackernoon.com/consensus-mechanisms-explained-pow-vs-pos-89951c66ae10.

8] Jimi S., "Blockchain: how mining works and transactions are processed in seven steps," *Medium*, May 2, 2018, accessed February 25, 2019, https://medium.com/coinmonks/how-a-miner-adds-transactions-to-the-blockchain-in-seven-steps-856053271476

9] See "Bitcoin Energy Consumption Index" and "Ethereum Energy Consumption," Digiconomist, accessed February 25, 2019, https://digiconomist.net/bitcoin-energy-consumption; https://digiconomist.net/ethereum-energy-consumption.

10] "Electricity Domestic Consumption," *Global Energy Statistical Yearbook 2018,* accessed February 25, 2019, https://yearbook.enerdata.net/electricity/electricity-domestic-consumption-data.html.

11] Tom DiChristopher, "No, Bitcoin Isn't Likely to Consume All the World's Electricity in 2020," *CNBC*, December 21, 2017, accessed February 25, 2019, https://www.cnbc.com/2017/12/21/no-bitcoin-is-likely-not-going-to-consume-all-the-worlds-energy-in-2020.html.

12] Mike Orcutt, "How Secure is Blockchain Really?" *MIT Technology Review*, April 25, 2018, accessed February 25, 2019, https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/

13] Alyssa Hertig, "The Latest Bitcoin Bug Was So Bad, Developers Kept Its Full Details a Secret," *CoinDesk*, September 21, 2018, accessed February 25, 2019, https://www.coindesk.com/the-latest-bitcoin-bug-was-so-bad-developers-kept-its-full-details-a-secret.

14] Josh Swihart, Benjamin Winston, and Sean Bowe, "Zcash Counterfeiting Vulnerability Successfully Remediated," *Zcash*, February 5, 2019, accessed March 1, 2019, https://z.cash/blog/zcash-counterfeiting-vulnerability-successfully-remediated.

15] "What Is an Eclipse Attack?" *Radix*, June 7, 2018, accessed February 25, 2019, https://www.radixdlt.com/post/what-is-an-eclipse-attack

16] Jake Frankenfield, "51% Attack," *Investopedia*, February 7, 2019, accessed February 25, 2019, https://www.investopedia.com/terms/1/51-attack.asp.

17] Jeff John Roberts, "Bitcoin Spinoff Hacked in Rare '51% Attack'," *Fortune*, May 29, 2018, accessed February 25, 2019, http://fortune.com/2018/05/29/bitcoin-gold-hack/.

18] Andrew Norry, "The History of the Mt Gox Hack: Bitcoin's Biggest Heist," *Blockonomi*, November 19, 2018, accessed January 25, 2019, https://blockonomi.com/mt-gox-hack/

19] Schumann, "Consensus Mechanisms Explained: POW vs. POS."

20] Miguel Castro and Barbara Liskov, "Practical Byzantine Fault Tolerance," *OSDI '99 Proceedings of the third symposium on Operating systems design and implementation,* 1999, 173–186, http://pmg.csail.mit.edu/papers/osdi99.pdf.

21] "Hyperledger," *The Linux Foundation*, accessed February 25, 2019, https://www.hyperledger.org/.

22] Brian Curran, "What is Practical Byzantine Fault Tolerance? Complete Beginner's Guide," *Blockonomi*, May 11, 2018, accessed February 25, 2019, https://blockonomi.com/practical-byzantine-fault-tolerance/.

23] Ibid.

24] Bitcoin Exchange Team, "Intel's POET (Proof of Elapsed Time) Blockchain Consensus Algorithm," *Bitcoin Exchange Guide*, June 18, 2018, accessed February 25, 2019, https://bitcoinexchangeguide.com/intels-poet-proof-of-elapsed-time-blockchain-consensus-algorithm/.

25] Priyeshu Garg, "What Is a Coin Burn? Beginner's Guide to Proof of Burn," *Blockonomi*, May 8, 2018, accessed February 25, 2019, https://blockonomi.com/proof-of-burn/.

26] "Proof Of Burn," *Bitcoin Wiki*, accessed February 25, 2019, https://en.bitcoin.it/wiki/Proof_of_burn.

27] Vitalik Buterin, "On Public and Private Blockchains," *Ethereum Blog*, August 6, 2015, accessed February 25, 2019, https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

28] Gideon Greenspan, "Smart Contracts and the DAO Implosion," *MultiChain*, June 22, 2016, accessed February 25, 2019, https://www.multichain.com/blog/2016/06/smart-contracts-the-dao-implosion/

29] "Decentralized. Immutable. Unstoppable." *Ethereum Classic*, accessed February 25, 2019, https://ethereumclassic.org/.

30] "Blockchain Speeds & the Scalability Debate," *Blocksplain*, February 28, 2018, accessed February 25, 2019, https://blocksplain.com/2018/02/28/transaction-speeds/.

31] Kieran Smith, "Vitalik — Ethereum En Route to a Million Transactions per Second," *Brave New Coin*, June 6, 2018, accessed February 25, 2019, https://bravenewcoin.com/insights/vitalik-ethereum-en-route-to-a-million-transactions-per-

second.

32] "Visa Inc at a Glance," *Visa*, data as of March 31, 2014, accessed February 25, 2019, https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf.

33] Estimate based on the fact that Visa handles 150 million transactions each day. Jan Vermeulen, "VisaNet – Handling 100,000 Transactions per Minute," *My Broadband*, December 17, 2016, accessed February 25, 2019, https://mybroadband.co.za/news/security/190348-visanet-handling-100000-transactions-per-minute.html.

34] Richard Lumb et al., "Why Distributed Ledger Technology Must Adapt to an Imperfect World" (Accenture, 2016) accessed February 25, 2019, https://www.accenture.com/t00010101T000000__w__/es-es/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf

35] Ibid.

36] Laura Shin, "Canada Has Been Experimenting With a Digital Fiat Currency Called CAD-COIN," *Forbes*, June 16, 2016, accessed January 25, 2019, http://www.forbes.com/sites/laurashin/2016/06/16/canada-has-beenexperimenting-with-a-digital-fiat-currency-called-cad-coin/#5eb84cdb1b0c; Marie Huillet, "China: Central Bank's Digital Currency Lab Launches Research Center in Eastern Province," *CoinTelegraph*, September 5, 2018, accessed April 4, 2019, https://cointelegraph.com/news/china-central-banks-digital-currency-lab-launches-research-center-in-eastern-province.

37] Francisco Memoria, "Turns out Venezuela's Oil-Backed Petro Cryptocurrency Is Real After All," *CCN*, January 28, 2019, accessed April 2, 2019, https://www.ccn.com/turns-out-venezuelas-oil-backed-petro-cryptocurrency-is-real-after-all.

38] Robert D. Atkinson, Daniel Castro, and Alan McQuinn, "ITIF Comments to the New York State Department of Financial Services on the Proposed BitLicense Framework" (Information Technology and Innovation Foundation, October 21, 2014), https://itif.org/publications/2014/10/21/itif-commentsnew-york-state-department-financial-services-proposed.

39] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System."

40] "Crypto Market Overview," *Coin Codex*, accessed February 25, 2019, https://coincodex.com/market-overview/.

41] "Cryptocurrency List," *CoinLore*, accessed February 25, 2019, https://www.coinlore.com/all_coins.

42] Alan McQuinn, Weining Guo, and Daniel Castro, "Policy Principles for Fintech" (Information Technology and Innovation Foundation, October 2016), http://www2.itif.org/2016-policy-principles-fintech.pdf

43] Dan Blystone, "Bitcoin Transactions Versus Credit Card Transactions," *Investopedia*, updated September 29, 2018, accessed February 12, 2019, https://www.investopedia.com/articles/forex/042215/bitcoin-transactions-vs-credit-card-transactions.asp; Data gathered from BitInfoCharts. "Bitcoin – Avg. Transaction Fee," *BitInfoCharts*, 3 month transaction average, accessed February 12, 2019, https://bitinfocharts.com/comparison/bitcoin-transactionfees.html#3m.

44] Eline Chivot, "5Q's for Amir Sarhangi, Vice President of Product at Ripple," *Center for Data Innovation*, March 13, 2019, accessed March 18, 2019, https://www.datainnovation.org/2019/03/5qs-for-amir-sarhangi-vice-president-of-product-at-ripple/.

45] See the Bitcoin Volatility Index for a measure of volatility. "Bitcoin Volatility Time Series," *The Bitcoin Volatility Index*, accessed August 3, 2016, https://btcvol.info/.

46] Justin Scheck and Shane Shifflett, "Hot Dirty Money Disappears Into the Black Hole of Cryptocurrency," *Wall Street Journal*, September 28, 2018, accessed February 25, 2019, https://www.wsj.com/articles/how-dirty-money-disappears-into-the-black-hole-of-cryptocurrency-1538149743.

47] Shannon Liao, "The U.S. Arrests Alleged Leader of $3.7 billion Cryptocurrency Pyramid Scheme," *The Verge*, March 8, 2019, accessed April 2, 2019, https://www.theverge.com/2019/3/8/18256662/us-onecoin-leader-arrested-cryptocurrency-pyramid-scheme.

48] Sherwin Dowlat, "Cryptoasset Market Coverage Initiation: Network Creation," *Bloomberg*, July 11, 2018, accessed March 1, 2019, https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ

49] Zarchary Coburn vs the Securities and Exchange Commission, November 8, 2018, accessed March 1, 2019, https://www.sec.gov/litigation/admin/2018/34-84553.pdf.

50] "Framework for 'Investment Contract' Analysis of Digital Assets," U.S. Securities and Exchange Commission, April 2, 2019, accessed April 4, 2019, https://www.bloomberg.com/opinion/articles/2019-04-04/token-sales-have-some-rules-now.

51] Ibid.

52] Paul Vigna and Alexander Osipovich, "Bots Are Manipulating Price of Bitcoin in 'Wild West of Crypto'," *Wall Street Journal*, October 2, 2018, accessed February 27, 2019, https://www.wsj.com/articles/the-bots-manipulating-bitcoins-price-1538481600.

53] Lauren Yates, "Meeting With Bitwise Asset Management, Inc., NYSE Arca, Inc., and Vedder Price P.C." U.S. Securities and Exchange Commission, March 20, 2019, accessed April 4, 2019, https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf.

54] Ibid.

55] Joseph Young. "Report: How Bots on Crypto Exchanges are Manipulating the Price of Bitcoin," *News BTC,* October 3, 2018, accessed March 1, 2019, https://www.newsbtc.com/2018/10/03/report-how-bots-on-crypto-exchanges-are-manipulating-the-price-of-bitcoin/.

56] For a summary of this idea and the European Union's experience, see Paul Krugman, "Revenge of the Optimum Currency Area," *New York Times*, June 24, 2012, accessed February 27, 219, http://krugman.blogs.nytimes.com/2012/06/24/revenge-of-the-optimum-currency-area/.

57] Vildana Hajric, "Bitcoin Hits Inflection Point With Volatility at 17-Month Low," *Bloomberg*, October 5, 2018, accessed February 27, 2019, https://www.bloomberg.com/news/articles/2018-10-05/bitcoin-hits-inflection-point-with-volatility-at-17-month-low

58] Preston Byrne "Stablecoins Are Doomed to Fail," *Prestonbyrne.com,* December 10, 2017, accessed March 1, 2019, https://prestonbyrne.com/2017/12/10/stablecoins-are-doomed-to-fail/.

59] Preston Byrne, "Basecoin (aka the Basis Protocol): The Worst Idea in Cryptocurrency, Reborn," *Prestonbyrne.com,* October 13, 2017, accessed March 1, 2019, https://prestonbyrne.com/2017/10/13/basecoin-bitshares-2-electric-boogaloo/

60] Importantly, this model is not actually how central banks manage the money supply. Central banks create money and buy assets with it. This type of stablecoin system creates an asset then gives it to token holders, which they can sell to new participants in the system. As Adam Smith, Institute Fellow Preston Byrne puts it, "Buying assets to create money versus selling assets to obtain money. There's a big difference." Ibid.

61] Preston Byrne, "Well I'll Be Damned: BTSX BitAsset Market Failure After Only 5 Days," *Prestonbyrne.com,* August 28, 2014, accessed March 1, 2019, https://prestonbyrne.com/2014/08/28/well-ill-be-darned/.

62] "Stability for the Blockchain," *Maker,* accessed March 1, 2019,https://makerdao.com/en/dai/.

63] Preston Byrne "Stablecoins Are Doomed to Fail."

64] "Gemini Dollar," *Gemini*, accessed March 1, 2019, https://gemini.com/dollar/.

65] Preston Byrne, "Thoughts on GeminiCoin," *Prestonbyrne.com,* August 28, 2014, accessed March 1, 2019, https://prestonbyrne.com/2018/09/10/thoughts-on-geminicoin/

66] Ibid.

67] "IBM Signs 6 Banking Clients for its Blockchain-based Payments Network; Announces Stablecoin Partnership," *The Block*, March 18, 2019, accessed March 22, 2019, https://www.theblockcrypto.com/tiny/ibm-signs-6-banking-clients-for-its-blockchain-based-payments-network-announces-stablecoin-partnership.

68] Mike Orcutt, "One of Crypto's Buzziest Stablecoins Might Be Heading for Trouble," *MIT Technology Review*, March 20, 2019, accessed March 22, 2019, https://www.technologyreview.com/s/613144/one-of-cryptos-buzziest-stablecoins-might-be-heading-for-trouble/.

69] Andy Greenberg, "FBI Says It's Seized $28.5 Million in Bitcoins From Ross Ulbricht, Alleged Owner of Silk Road," *Forbes*, October 25, 2013, accessed February 27, 2019, https://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/#6d2a47a02765.

70] Aziz, "Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies," *MastertheCrypto*, accessed February 27, 2019, https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/.

71] Cossack Labs, "Explain Like I'm 5: Zero Knowledge Proof (Halloween Edition)," *Hackernoon*, October 26, 2017, accessed February 27, 2019, https://hackernoon.com/eli5-zero-knowledge-proof-78a276db9eff

72] "Private Digital Currency," *Monero*, accessed March 1, 2019, https://www.getmonero.org/.

73] Sean Gallagher, "Researchers Say WannaCryp Operator Moved Bitcoins to 'Untraceable' Monero," *Arstechnica*, August 4, 2017, accessed February 25, 2019, https://arstechnica.com/gadgets/2017/08/researchers-say-wannacry-operator-moved-bitcoins-to-untraceable-monero/

74] "Leading Global Banks Together With TradeIX and R3 Pilot Blockchain Trade Finance Solution," *R3,* press release, February 21, 2018, accessed March 1, 2019, https://txfblob.blob.core.windows.net/assets/Marco_Polo_20170220.pdf.

75] Ian Allison, "94 Companies Join IBM and Maersk's Blockchain Supply Chain," *Coindesk*, August 6, 2018, accessed February 27, 2019, https://www.coindesk.com/90-companies-join-ibm-and-maersks-blockchain-supply-chain/.

76] JP Buntix, "Dubai Unveils Blockchain-Based Digital Silk Road Project," *The Merkle*, June 3, 2018, accessed March 1, 2019, https://themerkle.com/dubai-unveils-blockchain-based-digital-silk-road-project/.

77] "Cost Estimates of Foodborne Illnesses," *U.S. Department of Agriculture*, last updated May 15, 2017, accessed February 27, 2019, https://www.ers.usda.gov/data-products/cost-estimates-of-foodborne-illnesses.aspx#.VDW27r4mUfy.

78] Knut Alicke et al., "Blockchain Technology for Supply Chains—A Must or a Maybe?" (Mckinsey & Company, September 2017), accessed February 27, 2019, https://www.mckinsey.com/business-functions/operations/our-insights/blockchain-technology-for-supply-chainsa-must-or-a-maybe.

79] Michael Corkery and Nathaniel Popper, "From Farm to Blockchain: Walmart Tracks Its Lettuce," *New York Times*, September 24, 2018, accessed February 27, 2019, https://www.nytimes.com/2018/09/24/business/walmart-blockchain-lettuce.html.

80] Ibid.

81] Kim Nash, "Walmart Requires Lettuce, Spinach Suppliers to Join Blockchain," *Wall Street Journal*, September 24, 2018, https://blogs.wsj.com/cio/2018/09/24/walmart-requires-lettuce-spinach-suppliers-to-join-blockchain/.

82] Lucas Mearian, "Q&A: Walmart's Frank Yiannas on the Use of Blockchain for Food Safety," *Computerworld*, October 1, 2018, accessed February 27, 2019, https://www.computerworld.com/article/3309656/emerging-technology/qa-walmarts-frank-yiannas-on-the-use-of-blockchain-for-food-safety.html.

83] Frederick Reese, "Land Regidstry: A Big Blockchain Use Case Explored," *Coindesk*, April 19, 2017, accessed February 27, 2019, https://www.coindesk.com/blockchain-land-registry-solution-seeking-problem.

84] Gertrude Chavez-Dreyfuss, "Honduras to Build Land Title Registry Using Bitcoin Technology," *Reuters*, May 15, 2015, accessed February 27, 2019, https://in.reuters.com/article/usa-honduras-technology/honduras-to-build-land-title-registry-using-bitcoin-technology-idINKBN0O01V720150515.

85] John Mirkovic, "Blockchain Cook Countyâ€Š—â€ŠDistributed Ledgers for Land Records," *Illinois Blockchain Initiative*, May 31, 2017, accessed March 1, 2019, https://illinoisblockchain.tech/blockchain-cook-county-final-report-1f56ab3bf89.

86] Ibid.

87] Ibid.

88] Sharanya Haridas, "This Indian City Is Embracing BlockChain Technology—Here's Why," *Forbes*, May 5, 2018, accessed February 27, 2019, https://www.forbes.com/sites/outofasia/2018/03/05/this-indian-city-is-embracing-blockchain-technology-heres-why/.

89] Claudio Guarnieri, "Online Voting Is a Terrible Idea," *Motherboard,* June 9, 2017, accessed February 26, 2019, https://motherboard.vice.com/en_us/article/d3zywz/online-voting-is-a-terrible-idea; "Electronic Voting – Why It's Bad for Democracy," *National Election Defense Coalition*, accessed February 26, 2019, https://www.electiondefense.org/electronic-voting-why-its-bad-for-democracy.

90] Daniel Castro, "Stop the Presses: How Paper Trails Fail to Secure e-Voting" (Information Technology and Innovation Foundation, September 2007), http://www.itif.org/files/evoting.pdf.

91] Terry Nguyen, "West Virginia to Offer Mobile Blockchain Voting App for Overseas Voters in November Election," *Washington Post,* August 10 ,2018, accessed February 26, 2019, https://www.washingtonpost.com/technology/2018/08/10/west-virginia-pilots-mobile-blockchain-voting-app-overseas-voters-november-election/?utm_term=.2bc0199fee92.

92] Max Yakubowski, "South Korean Government to Test Blockchain Use for E-Voting System," *Coin Telegraph,* November 28, 2018, accessed February 26, 2019, https://cointelegraph.com/news/south-korean-government-to-test-blockchain-use-for-e-voting-system.

93] Nick Szabo, "Smart Contracts: the Building Blocks for Digital Markets," available on *True Value Metrics*, 1996, accessed on March 22, 2019, http://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf.

94] "Explore Decentralized Application," *State of the DAPPS*, accessed March 1, 2019, https://www.stateofthedapps.com/.

95] Natalia Karayaneva, "How A Smart Contract Replaced an Escrow Company in a $60K Deal," *Hackernoon*, October 17, 2017, accessed February 27, 2019, https://hackernoon.com/how-a-smart-contract-replaced-an-escrow-company-in-a-60k-deal-551ff7839044.

96] "Buy and Sell Freely," *Open Bazaar,* accessed March 1, 2019, https://openbazaar.org/.

97] "Changing the Way We Corroborate," Bounties Network, accessed March 4, 2019, https://bounties.network/

98] Scott Burger et al., "The Value of Aggregators in Electricity Systems," *MIT Center for Energy and Environmental Policy Research,* January 2016, accessed March 4, 2019, https://energy.mit.edu/wp-content/uploads/2016/01/CEEPR_WP_2016-001.pdf.

99] Ernest Moniz et al., "Promising Blockchain Applications for Energy: Separating the Signal From the Noise," (Energy Futures Initiative, July 2018), accessed March 3, 2019, https://static1.squarespace.com/static/58ec123cb3db2bd94e057628/t/5b4e59751ae6cf086c4450a5/1531861368631/EFI_Blockchain_July2018_FINAL+.pdf.

100] Jennifer Key, "DERs and Blockchain," *Steptoe*, June 24, 2018, accessed March 4, 0219, https://www.steptoepurpablog.com/2018/06/ders-and-blockchain/.

101] Chris Baraniuk, "Microgrids and the Blockchain Are Powering Our Energy Future," *Wired*, October 12, 2017, accessed April 1, 2019, https://www.wired.co.uk/article/microgrids-wired-energy.

102] Energy Blockchain Network, "Centralized vs. Decentralized Energy: The Case for DERs," *Energy Blockchain Network*, June 9, 2018, accessed March 4, 2019, https://medium.com/energy-blockchain-network-publication/centralized-vs-decentralized-energy-the-case-for-ders-9d7d29eea8e7.

103] "TenneT Unlocks Distributed Flexibility via Blockchain," TenneT, May 2, 2017, accessed March 4, 2019, https://www.tennet.eu/news/detail/tennet-unlocks-distributed-flexibility-via-blockchain/.

104] Ibid.

105] Alex Miller et al., "Welcome to the Future of Energy," *Grid+*, 2017, accessed March 4, 2019, https://gridplus.io/assets/Gridwhitepaper.pdf.

106] Robert Atkinson, Daniel Castro, and Alan McQuinn, "Comments to the U.S. Department of Justice on the ASCAP and BMI Consent Decrees" (Information Technology and Innovation Foundation, August 6, 2014), https://itif.org/publications/2014/08/06/itif-comments-ascap-and-bmi-consent-decrees.

107] Ibid.

108] Alan McQuinn, "Congress Hits Right Note on Music Modernization Act" (Information Technology and Innovation Foundation, May 16, 2019), accessed February 27, 2019, https://itif.org/publications/2018/05/16/congress-hits-right-note-music-modernization-act.

109] RightsLedger, "ASCAP Panel Examines Blockchain in Music," *Medium*, June 15, 2018, accessed March 4, 2019, https://medium.com/rightsledger/ascap-panel-examines-blockchain-in-music-25a8b6b1a926.

110] The Orchard, accessed March 4, 2019, https://www.theorchard.com/.

111] Mike Errico, "Touring Can't Save Musicians in the Age of Spotify," *New York Times,* January 25, 2016, accessed March 4, 2019, https://www.nytimes.com/2016/01/25/magazine/touring-cant-save-musicians-in-the-age-of-spotify.html.

112] Ian Allison, "Major Music Rights Societies Join Up for Blockchain Copyright Using IBM and Hyperledger," *International Business Times*, April 7, 2017, accessed March 4, 2019, https://www.ibtimes.co.uk/major-music-rights-societies-join-blockchain-copyrights-using-ibm-hyperledger-1615942.

113] RightsLedger, accessed March 4, 2019, https://www.rightsledger.io/.

114] Kirill Shilov, "Why Blockchain Might Not Be the Perfect Technology for the Music Industry," *Hackernoon*, November 24, 2018, accessed March 4, 2019, https://hackernoon.com/why-blockchain-might-not-be-the-perfect-technology-for-the-music-industry-936db6aa2b35.

115] Alysa Yamada, "Blockchain Isn't Enough to Solve the Authenticity of Physical Artworks," *Medium*, July 15, 2018, accessed March 4, 2019, https://medium.com/@alysayamada/blockchain-isnt-enough-to-solve-the-authenticity-of-physical-artworks-74a11b371050.

116] "The Cost of Fraud," *Associaion of Certified Fraud Examiners*, 2014, accessed March 7, 2019, https://www.acfe.com/rttn/images/cost-of-fraud-infographic.pdf

117] "Counterfeiting & Piracy (BASCAP)," *International Chamber of Commerce*, accessed March 7, 2019, https://iccwbo.org/global-issues-trends/bascap-counterfeiting-piracy/.

118] Samantha Rodocchia, "Fighting Fakes With Blockchain: How To Make Anti-Counterfeiting Methods Effective for Luxury Goods," *Forbes*, October 16, 2018, accessed March 7 ,2019, https://www.forbes.com/sites/samantharadocchia/2018/10/16/fighting-fakes-with-blockchain-how-to-make-anti-counterfeiting-methods-effective-for-luxury-goods/#5a8cbe99356b.

119] Qiuyun Shang, "Fighting Fake Drugs on the Blockchain," *New America*, April 25, 2018, accessed March 7 ,2019, https://www.newamerica.org/bretton-woods-ii/blockchain-trust-accelerator/around-the-blockchain-blog/fighting-fake-drugs-blockchain/.

120] "2016 Top Markets Report Pharmaceuticals," *U.S. International Trade Administration*, 2016, accessed March 7, 2019, https://www.trade.gov/topmarkets/pdf/Pharmaceuticals_Executive_Summary.pdf.

121] "1 in 10 Medical Products in Developing Countries is Substandard or Falsified," World Health Organization, news release, November 28, 2017, accessed March 7 ,2019, http://www.who.int/en/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified.

122] Drug Supply Chain Security Act (DSCSA), Pub.L. 113–54, 127 Stat. 587-640, (2013).

123] "Counterfeit Drugs in America: Crimes, Victims & Solutions," *The Partnership for Safe Medicines,* 2nd edition, March 2017, accessed March 7, 2019, https://www.safemedicines.org/wp-content/uploads/PSM_FP2_footnotes_secure-1.pdf.

124] IBM Research, "Using Blockchain to Prevent Counterfeit Drugs in Kenya," *Youtube*, July 27, 2017, accessed March 7, 2019, https://www.youtube.com/watch?v=11Z4-XYoZAE

125] "DHL and Accenture Unlock the Power of Blockchain in Logistics," *DHL*, news release, March 12, 2018, accessed March 7, 2019, http://www.dhl.com/en/press/releases/releases_2017/all/dhl_and_accenture_unlock_the_power_of_blockchain_in_logistics.html.

126] MediLedger, accessed March 7, 2019, https://www.mediledger.com/.

127] Angeline Mbogo, "How the Blockchain Can Prevent Drug Counterfeiting in Kenya," *Bitcoin Africa*, January 18, 2019, accessed March 7, 2019, https://bitcoinafrica.io/2018/01/18/blockchain-prevent-drug-counterfeiting-kenya/.

128] Brady Dale, "Non-Believable Tokens: The 7 Strangest Crypto Collectibles Explained," *CoinDesk*, August 20, 2018, accessed March 7 , 2019, https://www.coindesk.com/the-7-strangest-non-fungible-tokens-for-cryptos-collectors/.

129] CryptoKitties, accessed March 7 ,2019, https://www.cryptokitties.co/.

130] Jon Jordan, "CryptoKitties' Total Transactions Hits $25 Million," *Blockchain Gamer*, June 18, 2018, accessed March 7, 2019, https://www.blockchaingamer.biz/news/4137/cryptokitties-transactions-hits-25-million/

131] Daniel Castro and Jordan Misra, "The Internet of Things" (Center for Data Innovation, November 18, 2013), https://www.datainnovation.org/2013/11/the-internet-of-things/.

132] Alex Moskov, "How Identity of Things (IDOT) and IOT on the Blockchain Could Impact Autonomous Vehicles," *DataFloq*, March 28, 2018, accessed March 7, 2019, https://datafloq.com/read/identity-of-things-blockchain-autonomous-vehicles/4773.

133] "Lightweight Node," *Bitcoin wiki*, accessed March 7, 2019, https://en.bitcoin.it/wiki/Lightweight_node.

134] Serguei Popov, "The Tangle" (IOTA, April 30, 2018), accessed March 7, 2019, https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf.

135] Nick Marinos and Michael Clements, "Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach" (U.S. Government Accountability Office, September 7, 2018), accessed March 1, 2019, https://www.gao.gov/products/GAO-18-559.

136] Michael Graglia, Christopher Mellon, and Tim Robustelli, "The Nail Finds a Hammer: Self Sovereign Identity, Design Principles, and Property Rights in the Developing World" (New America, October 18, 2018), accessed October 30, 2018, https://www.newamerica.org/future-property-rights/reports/nail-finds-hammer/.

137] Yael Grauer, "A Critical Look at Sovereign Identity Startups," *BreakerMag*, September 20, 2018, accessed March 7, 2019, https://breakermag.com/a-critical-look-at-sovereign-identity-startups/.

138] "Partners," *Civic*, accessed March 7 ,2019, https://www.civic.com/solutions/partners/.

139] Grauer, "A Critical Look at Sovereign Identity Startups."

140] For example, see Jumio, accessed March 7, 2019, https://www.jumio.com/.

141] Daniel Castro, "Electronic Identification" (Information Technology and Innovation Foundation, September 2011), accessed February 27, 2019, http://www.itif.org/files/2011-e-id-report-final.pdf.

142] McQuinn, Guo, and Castro, "Policy Principles for Fintech."

143] Huw Jones, "Regulators Say New EU Cryptoasset Rules May be Needed," *Reuters*, January 9, 2019, https://www.reuters.com/article/us-eu-cryptoassets-regulation/regulators-say-new-eu-cryptoasset-rules-may-be-needed-idUSKCN1P316K.

144] Bhushan Akolkar, "China Officially Bans All Crypto-Related Commercial Activities," *Bitcoinist*, August 22, 2018, accessed March 8 ,2019, https://bitcoinist.com/china-officially-bans-crypto-activities/; Joseph Young, "No, China Has Not Legalized Nor Put an End to Bitcoin Ban; Inaccurate Reports," *Cryptoslate,* November 9, 2018, accessed March 8, 2019, https://cryptoslate.com/no-china-has-not-legalized-nor-put-an-end-to-bitcoin-ban-inaccurate-reports/

145] See Protiviti, Guide to U.S. Anti-Money Laundering Requirements FAQ, 6th ed., (Protiviti, 2014), https://www.protiviti.com/US-en/insights/guide-us-anti-money-laundering-requirements-faq-6th-ed.

146] Anti-Drug Abuse Act of 1998, Pub.L. 100–690, 102 Stat. 4181 (1988); The Foreign Corrupt Practices Act (1977), Pub.L. 95-213, 91 Stat. 1494 (1977).

147] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," *Financial Crimes Enforcement Network*, FIN-2013-6001, March 18, 2013, accessed March 8, 2019, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

148] U.S. Department of the Treasury Financial Crimes Enforcement Network, "FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger," news release, May 5, 2015, accessed March 8, 2019, https://www.fincen.gov/news_room/nr/pdf/20150505.pdf.

149] Crew Maloney, "Letter to Sen. Ron Wyden," *U.S. Department of the* Treasury, February 13, 2018, accessed March 8, 2019 https://coincenter.org/files/2018-03/fincen-ico-letter-march-2018-coin-center.pdf.

150] "Know Your Exchange (KYE) Report" (Coinfirm, March 2019), accessed April 4, 2019, https://coinfirm-prod.objects.frb.io/assets/Coinfirm_Exchange_Report_March_2019_Public.pdf.

151] Pete Rizzo, "CFTC Ruling Defines Bitcoin and Digital Currencies as Commodities," *CoinDesk*, September 17, 2015, accessed March 8, 2019, https://www.coindesk.com/cftc-ruling-defines-bitcoin-and-digital-currencies-as-commodities

152] U.S. Commodity and Futures Tradition Commission, "CFTC Orders Bitcoin Options Trading Platform Operator and Its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps Without Registering," news release, September 17, 2015, accessed March 8, 2019, https://www.cftc.gov/PressRoom/PressReleases/pr7231-15.

153] Jay Clayton, "Statement on Cryptocurrencies and Initial Coin Offerings," *U.S. Securities and Exchange Commission*, December 11, 2017, accessed March 8 ,2019, https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

154] Jay Clayton, "Statement on NASAA's Announcement of Enforcement Sweep Targeting Fraudulent ICOs and Crypto-asset Investment Products," *U.S. Securities and Exchange Commission*, May 22, 2018, accessed March 8 ,2019, https://www.sec.gov/news/public-statement/statement-nasaas-announcement-enforcement-sweep-targeting-fraudulent-icos-and.

155] "Framework for 'Investment Contract' Analysis of Digital Assets," U.S. Securities and Exchange Commission.

156] William Hinman, "Digital Asset Transactions" When Howey Met Gary (Plastic)," *U.S. Securities and Exchange Commission*, June 14, 2018, accessed March 8 ,2019, https://www.sec.gov/news/speech/speech-hinman-061418

157] "Response of the Division of Corporation Finance to TurnKey Jet, Inc." (U.S. Securities and Exchange Commission, April 2, 2019), accessed April 4, 2019, https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm.

158] Paragon Coin Inc., vs. U.S. Securities and Exchange Commission, November 16, 2018, https://www.sec.gov/litigation/admin/2018/33-10574.pdf

159] Paul Vigna and Dave Michaels, "Are ICO Tokens Securities? Startup Wants a Judge to Decide," *Wall Street Journal*, January 27, 2019, accessed January 30, 2019, https://www.wsj.com/articles/are-ico-tokens-securities-startup-wants-a-judge-to-decide-11548604800.

160] Nikhil Subba, "SEC Rejects Nine Proposals for Bitcoin ETFs," *Reuters*, August 22, 2018, accessed March 1, 2019, https://www.reuters.com/article/us-bitcoin-funds-etfs/sec-rejects-nine-proposals-for-bitcoin-etfs-idUSKCN1L802V.

161] "Virtual Currencies: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission," U.S. Senate Committee on banking, Housing, and Urban Affairs, February 6, 2018, accessed March 8, 2019, https://www.banking.senate.gov/hearings/virtual-currencies-the-oversight-role-of-the-us-securities-and-exchange-commission-and-the-us-commodity-futures-trading-commission.

162] Title 12 and 15 focuses on banks and banking and commerce and trade, respectively. 12 U.S.C. §§ 1 et seq., §§ 21 et seq., § 24., §§ 221 et seq., §§ 265-266, 1811-1832., §§ 1461-1470, §§ 1841-1850, §§ 4001-4010, §§ 5201 et seq., §§ 5301 et seq.; 15 U.S.C. §§ 1601 et seq., §§ 8301 et seq.

163] New York Codes, Rules and Regulations, Title 23. Department of Financial Services, Chapter 1. Regulations of the Superintendent of Financial Services, Part 200. Virtual Currencies, New York State Department of Financial Services, http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.

164] The Colorado Digital Token Act, S.B. 19-023 (2019).

165] U.S. Office of the Comptroller of the Currency, "OCC Begins Accepting National Bank Charter Applications From Financial Technology Companies," press release, accessed July 31, 2018, accessed March 21, 2019, https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-74.html.

166] Alan Kaplinsky, "State Regulators File Second Lawsuit Opposing OCC Fintech Charter," *Ballard Spahr LLP*, October 29, 2018, accessed March 21, 2019, https://www.consumerfinancemonitor.com/2018/10/29/state-regulators-file-second-lawsuit-opposing-occ-fintech-charter/.

167] "State Regulators Take First Step to Standardize Licensing Practices for Fintech Payments," *CSBS*, February 6, 2018, accessed March 8, 2019,https://www.csbs.org/state-regulators-take-first-step-standardize-licensing-practices-fintech-payments.

168] Peter Van Valkenburgh, "Food for Thought: A Federal Safe Harbor for Non-custodial Cryptocurrency Users," *CoinCenter*, September 7, 2016, accessed March 21, 2019, https://coincenter.org/entry/food-for-thought-a-federal-safe-harbor-for-non-custodial-cryptocurrency-users.

169] Robert Atkinson, Daniel Castro, and Alan McQuinn, "ITIF Comments to the New York Department of Financial Services on Bitlicenses" (Information Technology and Innovation Foundation, October 21 2014), http://www2.itif.org/2014-comments-nysdfs-bitlicenses.pdf.

170] New York Codes, Rules and Regulations, Title 23. Department of Financial Services, Chapter 1. Regulations of the Superintendent of Financial Services, Part 200. Virtual Currencies, New York State Department of Financial Services, http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.

171] Paul Vigna, "Coinbase's New Customer Incentive: Interest Payments, With a Crypto Twist," *Wall Street Journal*, March 29, 2019, accessed April 4, 2019, https://www.wsj.com/articles/coinbases-new-customer-incentive-interest-payments-with-a-crypto-twist-11553855400.

172] Blockchain Regulatory Certainty Act, H.R. 6974 (2018), 115th Cong (2018).

173] Stan Higgens, "U.S. Finance Regulators Form Crypto Working Group, Says Mnuchin," *CoinDesk*, accessed January 12, 2018, accessed March 8, 2019, https://www.coindesk.com/financial-stability-oversight-council-forms-crypto-working-group-says-mnuchin.

174] The Federal Trade Commission Act, 15 U.S.C. § 41 (1914).

175] Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), 12 U.S.C. 1042.

176] Megan Gray, "Understanding and Improving Privacy 'Audits' Under FTC Orders," (Stanford Center for Internet and Society, April 2018), accessed February 28, 2019, https://cyberlaw.stanford.edu/files/blogs/white%20paper%204.18.18.pdf.

177] Duane Pozza and Helen Wong, "Fintech Forum: A Closer Look at Marketplace Lending," *Federal Trade Commission Business Blog*, August 3, 2016, accessed March 22, 2019, https://www.ftc.gov/news-events/blogs/businessblog/2016/08/fintech-forum-closer-look-marketplace-lending.

178] U.S. Commodity Futures Trading Commission, "CFTC Orders Bitcoin Options Trading Platform Operator and Its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps Without Registering," news release, accessed September 17, 2015, accessed March 8, 2019,

https://www.consumerfinance.gov/about-us/newsroom/cfpb-warns-consumers-about-bitcoin/.

179] These were violations of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, often referred to as the "Dodd-Frank Act." U.S. Consumer Financial Protection Bureau, "CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices," news release, March 2, 2016, accessed March 8, 2019, http://www.consumerfinance.gov/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-datasecurity-practices/.

180] Jo Ann S. Barefoot, "Disrupting Fintech Law," Fintech Law Report 18, no. 2 (March 2015), accessed March 20, 2019, 12, https://static1.squarespace.com/static/535edb77e4b0cd207fff9e6e/t/554ff231e4b0261b84be36e4/1431302705880/Fintech1802_AA_Barefoot.pdf.

181] Regulation (EU) 2016/679 (General Data Protection Directive), OJ L 119, March 05, 2016, Articles 1-99, http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

182] Alan McQuinn, "Understanding Data Privacy," *Real Clear Policy*, October 25, 2018, accessed February 25, 2019, https://www.realclearpolicy.com/articles/2018/10/25/understanding_data_privacy_110877.html.

183] Alan McQuinn and Daniel Castro, "A Grand Bargain on Data Privacy Legislation for America" (Information Technology and Innovation Foundation, January 2019), http://www2.itif.org/2019-grand-bargain-privacy.pdf.

184] California Financial Information Privacy Act (CFIPA), California Civil Code § 4050-4060 (2004).

185] McQuinn and Castro, "A Grand Bargain on Data Privacy Legislation for America."

186] Daniel Castro and Robert Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy" (Information Technology and Innovation Foundation, September 2014), http://www2.itif.org/2014-crossborder-internet-policy.pdf.

187] Castro and Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy"; "Middle East and North Africa," *End Blasphemy Laws*, accessed March 1, 2019, https://end-blasphemy-laws.org/countries/middle-east-and-north-africa/.

188] Nigel Cory, "How Website Blocking Is Curbing Digital Piracy Without 'Breaking the Internet'" (Information Technology and Innovation Foundation, August 2016), http://www2.itif.org/2016-website-blocking.pdf.

189] The Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (1998).

190] Roman Matzutt et al., "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin" Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC). Springer, 2018, https://fc18.ifca.ai/preproceedings/6.pdf.

191] David Canellis, "Here's Why Bitcoin's Blockchain Has Blocks That Go Over the 1MB Limit," *The Next Web*, July 12, 2018, accessed March 1, 2019, https://thenextweb.com/hardfork/2018/07/12/bitcoin-block-size/.

192] Andrew Sward et al., "Data Insertion in Bitcoin's Blockchain," Computer Science: Faculty Scholarship & Creative Works, July 2017, https://digitalcommons.augustana.edu/cgi/viewcontent.cgi?article=1000&context=cscfaculty.

193] "Regulation of Cryptocurrency Around the World" (The Law Library of Congress, June 2018), accessed march 8, 2019, https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf.

194] "Notice 2014-21" U.S. Internal Revenue Service, 2014, accessed March 8, 2019, https://www.irs.gov/pub/irs-drop/n-14-21.pdf

195] Jerry Brito, "Bitcoin Taxation Is Broken. Here's How to Fix It." *CoinCenter*, April 12, 2017, accessed March 21, 2019, https://coincenter.org/entry/bitcoin-taxation-is-broken-here-s-how-to-fix-it.

196] Ibid.

197] Cryptocurrency Tax Fairness Act in 2017, H.R. 3708 (2017), 115th Cong. (2017).

198] Ross Cormack, "Legality of Gambling on the Blockchain," *Medium*, March 3, 2018, accessed March 8, 2019, https://medium.com/edgefund/legality-of-gambling-on-the-blockchain-26599785700f.

199] The Federal Wire Act of 1961, Pub. L. 87–216, 75 Stat. 491 (1961); the Unlawful Internet Gambling Enforcement Act (UIGEA) of 2006, 31 USC 5361-5366 (2006).

200] Illegal Gambling Business Act, 18 U.S.C. 1955 (1970).

201] "CFTC Fraud Advisories," *U.S. Commodity Futures Trading Commission*, accessed March 8, 2019, https://www.cftc.gov/ConsumerProtection/FraudAwarenessPrevention/CFTCFraudAdvisories/fraudadv_binaryoptions.html.

202] Augur, accessed March 8, 2019, https://www.augur.net/.

203] "FAQ," *Augur*, accessed March 8, 2019, https://www.augur.net/faq/

204] "Percentage of Total Market Dominance," CoinMarket Cap, accessed April 2, 2019, https://coinmarketcap.com/charts/.

205] Thibault Schrepel, "Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox," 3 Geo. L. Tech. Rev., June 11, 2018, updated October 6, 2018, https://poseidon01.ssrn.com/delivery.php (accessed March 8, 2019).

206] Ibid.

207] Atkinson, Castro, and McQuinn, "ITIF Comments to the New York Department of Financial Services on Bitlicenses."

208] Shelby Livingston, "HHS Using Blockchain to Streamline Contract Procurement," *Modern Healthcare*, February 9, 2019, accessed March 8, 2019, https://www.modernhealthcare.com/article/20190209/TRANSFORMATION02/190209950/hhs-using-blockchain-to-streamline-contract-procurement.

209] "GSA Schedules Frequently Asked Questions," U.S. General Services Administration, accessed February 25, 2018, http://www.gsa.gov/portal/content/203021.

210] Ibid.

211] Ibid.

212] McQuinn, Guo, and Castro, "Policy Principles for Fintech."

213] JD Alois, "CFTC Advocates Use of Blockchain for Swap Regulatory Reform," *Crowdfund Insider*, April 26, 2018, accessed March 8, 2019, https://www.crowdfundinsider.com/2018/04/132633-cftc-advocates-use-of-blockchain-for-swap-regulatory-reform/.

214] House Agriculture GOP, "Full Committee – Public Hearing RE: Examining the Upcoming Agenda for the CFTC," *Youtube*, July 25, 2018, accessed March 8, 2019, https://www.youtube.com/watch?v=indHENC2_2U&feature=youtu.be&t=57m15s

215] Commodity Futures Trading Commission Research and Development Modernization Act, H.R. 6121 (2018), 115th Congress (2017-2018).

216] Peter L. Singer, "Federally Supported Innovations: 22 Examples of Major Technology Advances That Stem From Federal Research Support" (Information Technology and Innovation Foundation, February 2014), http://www2.itif.org/2014-federally-supported-innovations.pdf.

217] "UETA and ESIGN Act," *DocuSign*, accessed March 8, 2019, https://www.docusign.com/learn/us-electronic-signature-laws-and-history.

218] Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 96 (2000).

219] Riley Svikhart, "Blockchain's Big Hurdle," *Stanford Law Review*, November 2017, accessed March 8, 2019, https://www.stanfordlawreview.org/online/blockchains-big-hurdle/

220] Ian Calderon, "Calderon Bill Providing Legal Certainty for Use of Blockchain Technology Goes to Governor," California Legislature, press release, August 27, 2018, accessed April 22, 2019, https://a57.asmdc.org/press-releases/calderon-bill-providing-legal-certainty-use-blockchain-technology-goes-governor.

221] Nikhilesha De, "Arizona Governor Signs Latest Blockchain Bill Into Law," *Coindesk*, April 5, 2018, accessed October 28, 2018, https://www.coindesk.com/arizonas-governor-signs-latest-blockchain-bill-into-law.

222] Svikhart, "Blockchain's Big Hurdle."

223] McQuinn, Guo, and Castro, "Policy Principles for Fintech."

224] Brian Fung, "U.S. Regulators Say They Don't Have Enough Power Over Cryptocurrency Exchanges," *Washington Post*, February 6, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/02/06/u-s-regulators-say-they-dont-have-enough-power-over-cryptocurrency-exchanges/?utm_term=.53e0e2ccb213.

225] Barbara Underwood, "Virtual Markets Integrity Initiative" (New York State Attorney General's Office, September 2018), accessed March 8, 2019, https://ag.ny.gov/sites/default/files/vmii_report.pdf.

226] "State Regulators Take First Step to Standardize Licensing Practices for Fintech Payments."

227] Nader Al-Naji et al., "Basis," December 13, 2018, accessed March 8, 2019, https://www.basis.io/.

228] Sweetbridge, "The First Lending Platform Backed by Tokenized Titled Assets in the United States," *Medium,* November 2, 2018, accessed March 8, 2019, https://blog.sweetbridge.com/the-first-lending-platform-backed-by-tokenized-titled-assets-in-the-united-states-22d694d9366a.

229] Kyle Torpey, "CFTC Advisory Committee Recommends Creation of Virtual Currency Subcommittee," *Bitcoin Magazine*, February 15, 2018, accessed March 8, 2019, https://bitcoinmagazine.com/articles/cftc-advisory-committee-recommends-creation-virtual-currency-subcommittee/.

[230] "Regulatory Sandbox – Cohort 4," *Financial Conduct Authority*, March 7, 2018, accessed March 8, 2019, https://www.fca.org.uk/firms/regulatory-sandbox/regulatory-sandbox-cohort-4-businesses.

[231] "MAS Proposes New Regulatory Sandbox With Fast-Track Approvals," *Monetary Authority of Singapore*, November 14, 2018, accessed March 8, 2019, http://www.mas.gov.sg/News-and-Publications/Media-Releases/2018/MAS-Proposes-New-Regulatory-Sandbox-with-FastTrack-Approvals.aspx.

[232] Arizona Attorney General Mark Brnovich, "Arizona Becomes First State in U.S. to Offer Fintech Regulatory Sandbox," news release, 2018, accessed March 8, 2019, https://www.azag.gov/press-release/arizona-becomes-first-state-us-offer-fintech-regulatory-sandbox.

[233] Bureau of Consumer Financial Protection, "Policy on No-Action Letters and the BCFP Product Sandbox," Federal Register, December 13, 2018, accessed March 8, 2019, https://www.federalregister.gov/documents/2018/12/13/2018-26873/policy-on-no-action-letters-and-the-bcfp-product-sandbox.

[234] Daniel Castro, "Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising" (Information Technology and Innovation Foundation, December 2011), http://www.itif.org/files/2011- self-regulation-online-behavioral-advertising.pdf.

[235] Ibid.

[236] Lydia Beyoud, "Crypto Self-Regulatory Body Proves to Be No Easy Feat," *Bloomberg News*, May 16, 2018, accessed January 28, 2019, https://www.bna.com/crypto-selfregulatory-body-n73014475994/.

[237] Omar Faridi, "Japan's Virtual Currency Exchange Association (JVCEA) Now Authorized As Self-Regulatory Body," *CryptoGlobe*, October 24, 2018, accessed January 28, 2019, https://www.cryptoglobe.com/latest/2018/10/japan-s-virtual-currency-exchange-association-jvcea-now-authorized-as-self-regulatory-body/.

[238] Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene" (Information Technology and Innovation Foundation, February 2015), http://www2.itif.org/2015-howwhenregulators-intervene.pdf, (accessed January 28, 2019).

[239] Daniel Castro and Alan McQuinn, "Comments to FTC on Nomi Technologies, Inc." (Information Technology and Innovation Foundation, May 2015), accessed October 29, 2018, https://itif.org/publications/2015/05/26/comments-ftc-nomi-technologies-inc.

[240] Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene" (Information Technology and Innovation Foundation, February 2015), accessed October 29, 2018, http://www2.itif.org/2015-how-when-regulators-intervene.pdf.

[241] Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law" (Information Technology and Innovation Foundation, March 2016), accessed October 29, 2018, https://itif.org/publications/2016/03/14/unlocking-encryption-information-security-and-rule-law.

[242] Regulation (EU) 2016/679 (General Data Protection Directive), Article 17.

[243] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub.L. 115-164.

[244] Kerri Lemoie, "Blockchain and The Right to Be Forgotten," *Badgechain*, January 4, 2018, accessed March 1, 2019, http://badgechain.com/badgechain-newsletter-16-blockchain-and-the-right-to-be-forgotten/.

[245] Pub. L. No. 105-304, 112 Stat. 2860 (1998); "United States-Mexico-Canada Agreement," Office of the U.S. Trade Representative, accessed March 8, 2019, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement.

[246] Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" (Information Technology and Innovation Foundation, May 2017), http://www2.itif.org/2017-cross-border-data-flows.pdf.

[247] Ibid.

[248] Regulation (EU) 2016/679 (General Data Protection Directive).

[249] Castro and Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy."

[250] "The Global Standard Setter for Securities Markets Regulation," *OICU-IOSCO*, accessed April 1, 2019, https://www.iosco.org/.

ABOUT THE AUTHORS

Alan McQuinn is a senior policy analyst at the Information Technology and Innovation Foundation. He writes and speaks on a variety of issues related to information technology and Internet policy, such as cybersecurity, privacy, blockchain, fintech, e-government, Internet governance, intellectual property, and aerospace. He was previously a telecommunications fellow for Representative Anna Eshoo (D-CA). McQuinn graduated from the University of Texas at Austin with a B.S. in public relations and political communications and a minor in Mandarin Chinese.

Daniel Castro is vice president of ITIF and director of ITIF's Center for Data Innovation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Castro worked as an IT analyst at the Government Accountability Office, where he audited IT security and management controls at various government agencies. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

For more information, visit us at itif.org.