FinTech

Blockchain

Distributed ledger technology and designing the future

ReedSmith

Driving progress
through partnership

Contents

Foreward by the Chamber of Digital Commerce vi

The mysterious origins of blockchain 1

Blockchain 101 5

- How it works 5
- Digital currencies or “cryptocurrencies” 7
- Advantages of blockchain / DLT 7
- Disadvantages of blockchain / DLT 8
- Open vs. closed blockchains 10
- Summary 11

Smart contracts 13

- What they are 13
- Advantages of smart contracts on blockchains 13
- Disadvantages of smart contracts 14
- Smart contracts and derivatives 15

U.S. regulatory landscape 17

- State regulation 18
- Federal regulation and guidance 24
- Enforcement 30
- Conclusion 31

International regulatory landscape 33

- Europe 34
- Asia 38
- The Americas 40
- Middle East 40
- Africa 43

Insuring digital currency and digital currency business 45
Insurance and underwriting issues 47
Potential insurance coverage under traditional policies 47
Cyberattacks and ransomware 47
Financial institution bonds and commercial crime policies 48
D&O Insurance 49
E&O insurance 50
Kidnap and ransom (K&R) insurance 51
The bottom line 51
Applications in capital markets 53
Greater efficiencies 54
More security and transparency 55
Tokenizations 60
Potential risks 60
Blockchain innovation in the energy, commodities, shipping and trade finance industries 63
Energy producers and consumers 64
Energy trading 65
Shipping 67
Trade finance 69
Privacy and re-identification on the blockchain 73
Privacy 73
Psyeudonymity concerns 75
Industry-specific privacy concerns 76
Smart contracts 77

Intellectual Property 79
Bitcoin's open source license 79
Other blockchain application licenses 80
The rise of blockchain patents 80
Social impact, responsibility and media 83
Lowered transaction fees mean more money for causes 83
Greater transparency 83
Access to financial services 84
Financial empowerment 84
Initial/Independent coin offerings (ICOs) 85
Blockchain, media and advertising 86
Social media 87
Improving governance and minimizing corruption 87
Corporate social responsibility 87
Summary 87

Closing note 89
Glossary of terms 91
Key contacts 96
Endnotes 98

CHAMBER OF DIGITAL COMMERCE

Foreward

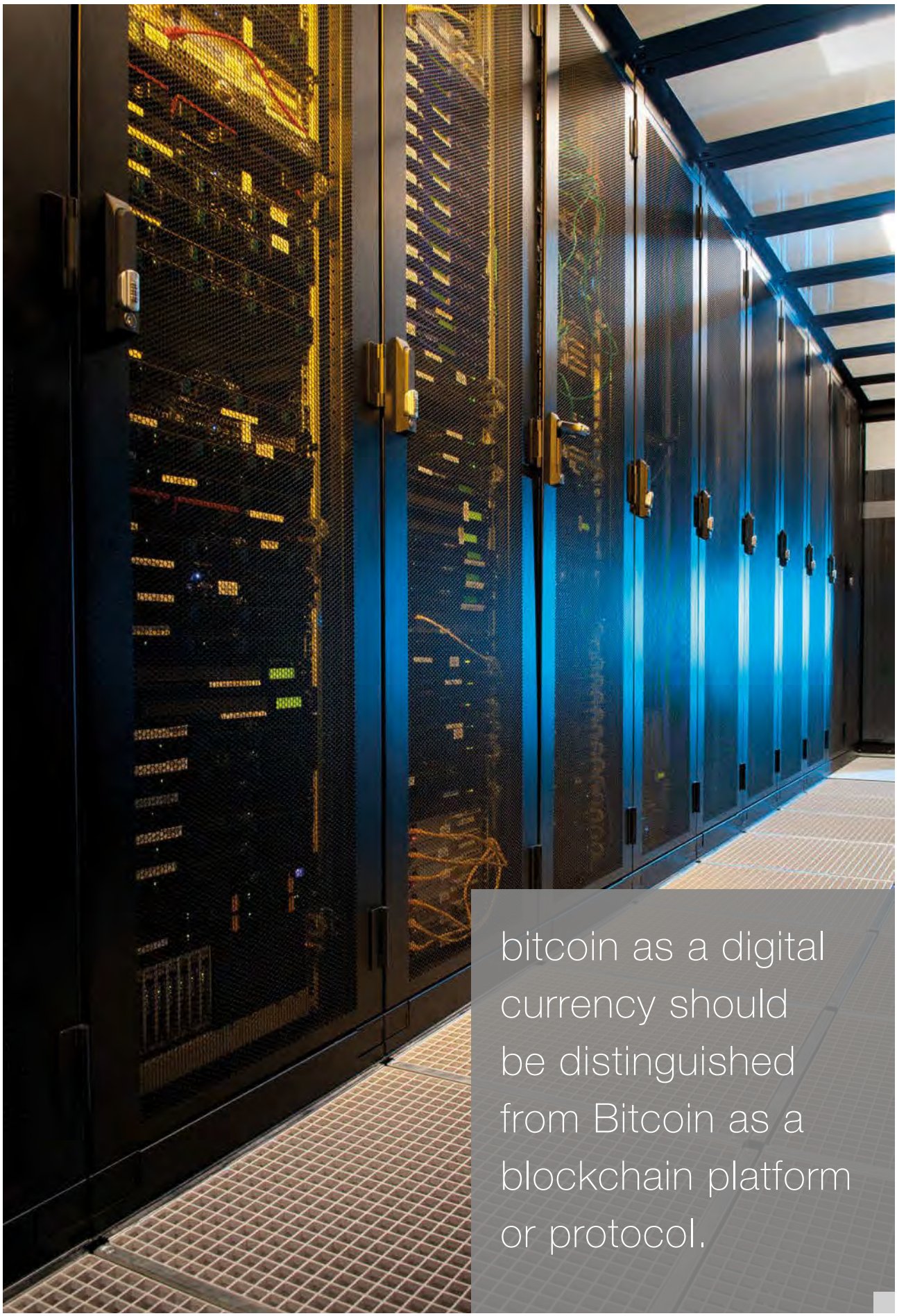
by the Chamber of Digital Commerce

We commend our good friends at Reed Smith for putting together this comprehensive compendium of U.S. federal and state, as well as non-U.S. country, laws and developments impacting the blockchain and virtual currency ecosystem. Navigating the regulatory requirements is complex given the numerous government agencies that have claimed jurisdiction over activities using blockchain technology. With the increased activity by federal regulators in particular, it is more important than ever to have law firms advise on the legal and regulatory landscape both in the United States and abroad.

Many of the companies in the blockchain space are trying to solve for a problem – whether it be for digital identity, the efficient distribution of loans and micropayments, or better tracking supply channels, to name a few. Often, they are technologists who may not be thinking of the intricacies of regulation in the industry. Or they may be business veterans, who are acutely aware of the pitfalls of legal and compliance requirements, and need a go-to firm to advise them on the do's and don'ts currently affecting their intended industry. While innovators are blazing new trails, there are many areas of the law that are unclear and companies must make sensible judgments in achieving compliance. Having a strong understanding of the legal landscape - as well as history of how we got here - is key to building a successful company in the blockchain sector.

Reed Smith's document is an important resource for participants in the blockchain ecosystem, laying out the foundation for regulatory oversight and then diving in to specific use cases and geographies to help guide this industry to success in a regulated environment. We have too often seen sensational headlines drive public perception of this industry. Setting out this information in a cohesive and understandable format is beneficial for everyone. As a member of our Lawyers Committee, Reed Smith is particularly well-placed to present its birds'-eye view of these developments.

As noted in the document, many gray areas remain within this legal landscape. As new digital assets, they do not always fall neatly into existing regulatory guidelines. Working with our membership, The Chamber of Digital Commerce identifies these gaps, and, where appropriate, advocates for agency or Congressional action to grow the digital asset and blockchain industry in a responsible environment. We rely on our membership to inform our views and drive our mission. Reed Smith has been an important member and valued resource in this space, and this document is clear evidence of the breadth of their abilities. We support their efforts to bring a comprehensive legal perspective to the industry.



bitcoin as a digital currency should be distinguished from Bitcoin as a blockchain platform or protocol.

The mysterious origins of blockchain

Introduction

Although the following chapters are mostly devoted to informing and enlightening the reader about the potential of cryptocurrencies* and the underlying blockchain technology, the origins of these developments are somewhat shrouded in mystery.

Halloween 2008 may have been a particularly frightening one, as the world economy was facing its most dangerous crisis since the Great Depression. Yet, it also happened to be the day that Bitcoin, the most widely used cryptocurrency to date, was introduced in a rather simple and unassuming email to several hundred members of an obscure mailing list comprising cryptography experts and enthusiasts.

The sender, known only by the pseudonym "Satoshi Nakamoto", wrote: "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party," followed by directions to the link http://www.bitcoin.org/bitcoin.pdf—a nine-page white paper about a peer-to-peer trustless system of digital "currency" that purports to solve the problem of double-spending.

After first becoming operational in January 2009, Bitcoin and its progeny have exploded. Exactly seven years after Nakamoto sent his or her initial, enigmatic email, the October 31, 2015, cover of *The Economist* featured an article on blockchain (the technology underlying Bitcoin), dubbing it "the trust machine."

More recently, *Fortune* extensively featured the rise of Bitcoin in its August 22, 2017 article:[1]

> "Finance is the most obvious extension of blockchain tech, given the monetary roots of Bitcoin. Trade finance, security clearance and settlements, cross-border payments, and insurance are all areas that could be overhauled and made more seamless. Microsoft is collaborating with Bank of America on a blockchain to digitize and automate the money flow around trades. HSBC, ING, U.S. Bank, and eight other banks recently completed a prototype application for the same purpose on R3's Corda ledger. Northern Trust, the asset management firm, is using Hyperledger Fabric for private-equity deal record keeping. And Ripple built a system to rival the SWIFT interbank money-transferring service. In a hotly competitive sector where

* Please refer to the Glossary for a list of definitions.

The application of the blockchain is anticipated to extend far beyond financial services

customers demand faster transactions and lower costs, the rewards of building the best blockchain mousetrap could be vast—the penalties for missing out, proportionately painful."

It is worth noting that bitcoin as a digital currency should be distinguished from Bitcoin as a blockchain platform or protocol. The distinction is analogous to that of an individual email versus the SMTP protocol through which the email is sent. Blockchain technology, which is described below, provides a cryptographically secured ledger that can be examined by all authorized parties, but cannot be changed.

Though Nakamoto initially collaborated with developers on what has been called a revolutionizing innovation, his participation ended in mid-2010, and in April 2011, he completely disappeared with the final words, "I've moved onto other things."

Though we may never discover the originator of Bitcoin, we are left with a rapidly developing open source technology that continues to find increasing mainstream acceptance, and simply cannot be ignored.

In fact, we have seen every sign that blockchain technology will be widely adopted in various industries. For example, the Hyperledger Project provides open source blockchain software that can be adapted to various applications. Intel has joined IBM, Digital Asset Holdings, and others in providing code and support for this project. Also, Digital Asset Holdings has collaborated with the Depository Trust and Clearing Corporation (DTCC) to test and build a blockchain-type distributed ledger to track and settle financial assets. The R3 consortium is a group of FinTech companies and large banks that are developing a financial grade open source distributed ledger platform known as Corda. Delaware recently passed legislation that allows Delaware chartered companies to maintain their stock ledgers via DLT.[2] Arizona passed a law clarifying that so called "smart contracts" made in computer code on a blockchain are enforceable.[3] Companies as diverse as Barclays, Depository Trust & Clearing Corp. and the Australian Stock Exchange are aggressively developing the ability to settle major financial transactions in this manner.[4]

The blockchain has also garnered attention from government agencies and regulators. For example, the U.S. Office of Comptroller of Currency (OCC) has proposed a framework where FinTech companies could apply for a special-purpose national bank charter, and has released a white paper posing an approach for overseeing experiments conducted by banking institutions with new technologies, such as blockchain protocols and applications. As discussed below, regulators in other countries and the European Union are also paying attention.

The application of the blockchain is anticipated to extend far beyond financial services to include various applications of authentication, supply chain management, data storage, real property records, digital content ownership verification, and business process management. Experimentation with the technology has only just begun.

What makes blockchain interesting is that it is a trustless system.

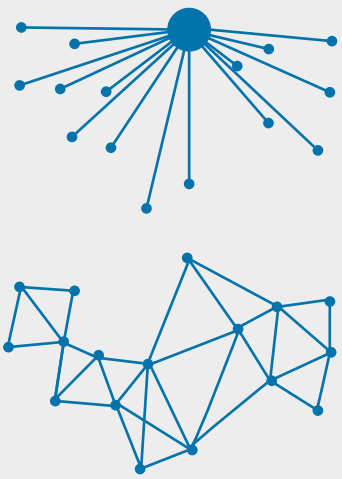
Blockchain 101

A blockchain is a cryptographically secured database of a continuously growing list of data records that is shared by all parties participating in an established, distributed network of computers. What makes blockchain interesting is that it is a trustless system. That is, blockchain makes it possible for participants that are not necessarily known to each other to transfer a digital asset without the requirement of any third-party validation. This chapter discusses in greater detail how the blockchain algorithm works to help you consider its greater potential.[5]

How it works

A **blockchain,**[6] also known as distributed ledger technology (DLT), is nothing more than a digital record, or ledger, of transactions. Unlike a traditional ledger, however, a blockchain is stored collectively by all of the participants on its network. Each transaction is stored with others in a unit of data called a **block**, and, as the name "blockchain" suggests, those blocks securely link to one another, forming a "chain" of records going all the way back to the very beginning of the ledger.

To participate in a blockchain network, a user must operate a software client that will connect it to that blockchain. The software client allows the user to record transactions, and also lends computing power to the



Adapted from loptio: https://github.com/ioptio/design/blob/master/networks/networks.png

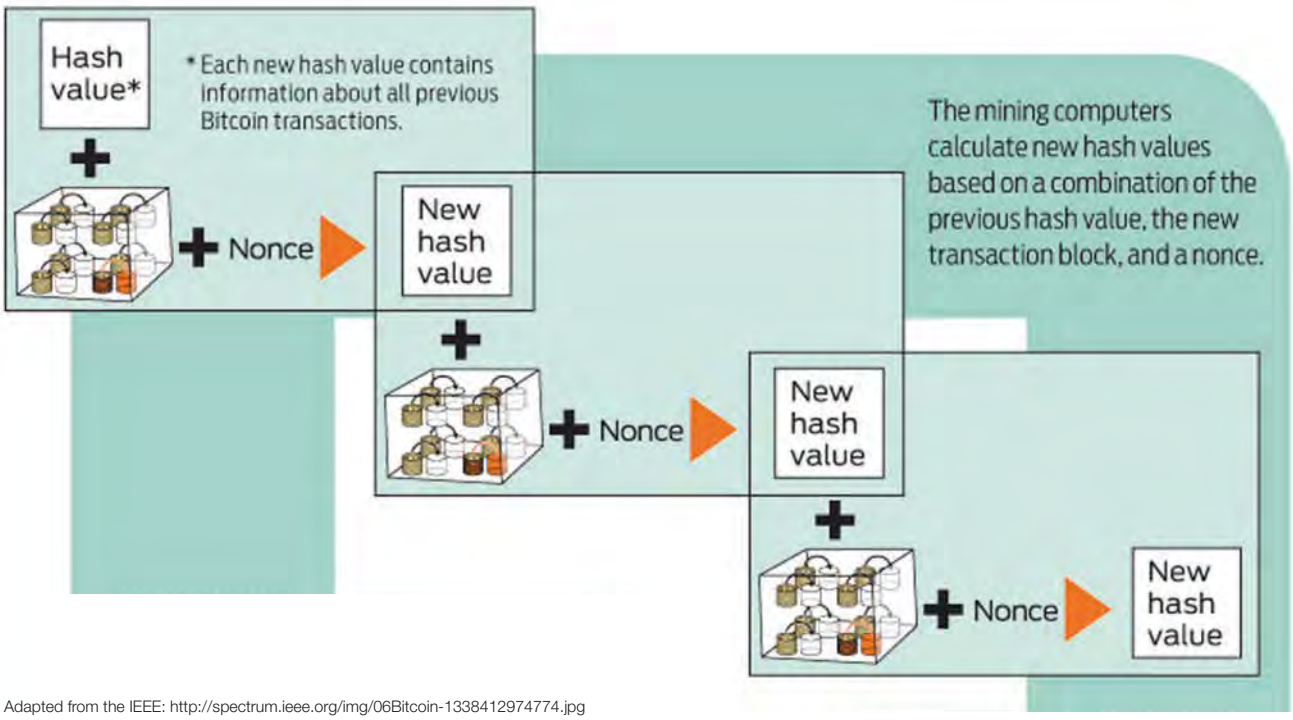
network to help build new blocks of records.

Various mechanisms exist for reaching global decentralized consensus on the blockchain as to the legitimacy of transactions broadcast to nodes on the network. For example, the Bitcoin blockchain has a proof-of-work consensus algorithm. Participants build new blocks of records by investing computer time (i.e., performing work) to solve complex mathematical problems. These new records are only added to the ledger when a majority of participants have double-checked the work of the person who wants to add it (i.e., "proof of work").

When a user wishes to transfer a digital asset to another user, the user and its counterparty broadcast cryptographically secured digital signatures and the details of their transaction to nearby peers on the network. The users are identified in the transaction by their public keys; this is termed "**pseudonymity**." When a peer participant solves the mathematical puzzle required for the next block, these pending transactions may now be recorded into a block. That new block is then double-checked by other members of the network until a majority agrees that it is correct. Once a majority consensus is achieved, the new block is added to the chain, and the pending transactions are recorded in the ledger.

Though the above summary is actually a simplification of the process, this is how blockchain allows a network of strangers to collectively maintain an accurate ledger of secure online records for any type of transaction, without the need for a trusted third party to act as a middleman.

As time goes on, more and more blocks of records are added to the blockchain, each one securely referencing the next. This is important because if someone wanted to go back and change a transaction on the ledger – to cook the digital books – she would not only have to re-solve the mathematical puzzle allowing her to create a fraudulent block, but she would also have to re-solve every subsequent block in the blockchain. Even worse for the fraudster, she would have to convince a majority of network participants to accept these fake blocks before the next legitimate participant added the next real block. The sheer volume of work and speed required make it extremely difficult to



Adapted from the IEEE: http://spectrum.ieee.org/img/06Bitcoin-1338412974774.jpg

alter transactions on a blockchain. This means that after a certain number of new blocks are added, the parties to a transaction can be well-assured that the transaction is considered final – not only by themselves, but also by the entire community of participants on the network. It is precisely this assurance that allows blockchain participants to trust the ledger itself, even though they do not necessarily trust (or know) their fellow participants on the network.

Digital currencies or "cryptocurrencies"

Digital currencies, also known as "cryptocurrencies,"[7] have gained significant attention since the introduction of Bitcoin in 2009. They offer a new medium of exchange and store of value created by and for the Internet that could potentially democratize the very idea of money itself.

Bitcoin was the first cryptocurrency, but hundreds of other cryptocurrencies have followed. Essential to its operation are two underlying technologies: public key cryptography and peer-to-peer networking.

- Public key cryptography is the use of digital signatures to secure information. These signatures consist of a public key, which is known by everyone, and a private key, known only by its owner.
- Peer-to-peer networking is a way to organize the flow of information among equal participants on a network, rather than relying on a central authority.

Bitcoin secures transactions between currency users with digital signatures, and then requires verification over a peer-to-peer network. Thus, when spending bitcoins[8], you sign the transaction with your private key to prove you own the bitcoin you want to spend. Then, your public key and the details of the transaction are published to a public ledger so that everyone knows that your bitcoin has changed hands. This public ledger is constantly being verified by the members of Bitcoin's peer-to-peer network to ensure that each bitcoin is spent only once, and is held by its verifiable owner. As such, Bitcoin replaces trust with mathematical proof and accountability among currency users themselves, thereby doing away with a central authority to monitor the ledger, or trusted third parties to clear transactions.

Digital currencies, also known as "cryptocurrencies," have gained significant attention since the introduction of Bitcoin in 2009.

Unlike a digital file on your computer, a bitcoin cannot be copied and pasted infinitely. It can only be transferred, and transferred only once, by signing the transaction with your private digital key, and recording the transaction on a shared public ledger.

Not only did Bitcoin solve the so-called "double spending" problem, where currency risked being spent more than once without the involvement of a middleman, but just as importantly, Bitcoin, owing to this middleman elimination, also cut down the time required to verify and finalize transactions from what can take several days in a traditional system, to a matter of minutes. This enables significant efficiencies and the growth of tremendous opportunities.

Advantages of blockchain / DLT

Distributed ledgers solve important problems in Internet commerce. Chief among them is the problem of double spending, where two transactions draw upon the same underlying asset. By requiring every transaction to be

at least partly public, distributed ledgers dramatically increase counterparty trust. Moreover, because blockchain requires transaction verification and consensus to record new transactions, it is very difficult for fraudsters to tamper with digital records to steal or re-spend assets. However, there have been several notable and large scale episodes of hackers successfully accessing the digital wallets of cryptocurrency holders resulting in the theft of currency from holders.

Because blockchain networks are peer-to-peer and do not require a third-party middleman to facilitate transactions between two parties, transactions are conducted, recorded, and made available to all users immediately, significantly increasing efficiency by cutting wait-time and lowering transaction costs. Transactions recorded on a blockchain are also generally immutable, and their details are visible to all users with access to it, allowing for full transparency and in turn promoting user accountability.

Blockchain also helps achieve certainty in the concept of digital ownership itself. A consummate problem with digital information is that it is freely transferable and may be copied. This means that possession cannot be equated with ownership. Merely having a copy of a file does not include the "right to exclude" – a touchstone built right into the concept of property. Distributed ledgers make proving the ownership of a digital asset more like performing a real property title search. Like the grantor-grantee index in land records, the blockchain records every transaction involving a particular digital asset. The advantage of blockchain over other forms of exclusive digital ownership, like encryption at rest,[9] is that there is always a record that reflects not only the current possession of the asset, but also the history of rightful ownership going all the way back to the digital asset's creation.

Disadvantages of blockchain / DLT

Like all technical solutions, the blockchain algorithm reflects certain tradeoffs. Because of latency and scalability issues, many current blockchain applications put severe limits on the size of each new block of

7

the number of payments per second the Bitcoin network can process

records. This limits the frequency with which a blockchain network can process transactions. For example, the Bitcoin network can only process seven payments per second, while major credit card providers can handle more than 1,400. This has caused the Bitcoin blockchain to experience increasing transaction delays, mostly because of the rapidly increasing number of network participants on its ledger. Scalability is a topic of concern that has been hotly debated within the blockchain community, with many disagreeing on the best method and approach to deal with the problem moving forward.

While scalability has been largely an issue of focus in the Bitcoin realm, many are concerned about how scaling will affect current and future blockchain-backed technology.

Ethereum for example, is a decentralized distributed ledger serving as a platform on which software developers to create and run blockchain-based applications. Ether is the value token of the Ethereum blockchain. The Ethereum blockchain has suffered similar network speed issues because of a spike in transactions and user congestion, raising the question of whether it or any other user-heavy blockchain will ever be able to adequately scale to accommodate and support a vastly growing user base.

Because scalability is an issue that is generally on-going when it comes to technology, and one that is more often resolved closer to when it actually becomes an issue, many are not concerned and are confident in the success of the numerous methods and technologies being developed to tackle the Bitcoin blockchain's and other DLT's current scalability problems. However,

designers of applications that leverage blockchain should carefully consider factors such as block size, the proof of work required to verify blocks, and the expected number of participants on a blockchain, to ensure the ledger operates efficiently and effectively.

Blockchain also relies heavily on public key cryptography to identify users and permit access to assets tracked through the ledger. For this reason, key security is of increased concern. If a user's private key is lost or stolen, the user has lost access to his or her assets on the blockchain forever. For example, as many as 4 percent of bitcoins have been rendered permanently ownerless because users have misplaced their digital keys. Future applications of blockchain, especially in private or semi-private contexts, should consider employing multi-factor authentication or digital certificates to safeguard the cryptographic keys used to identify rightful owners and permit access.

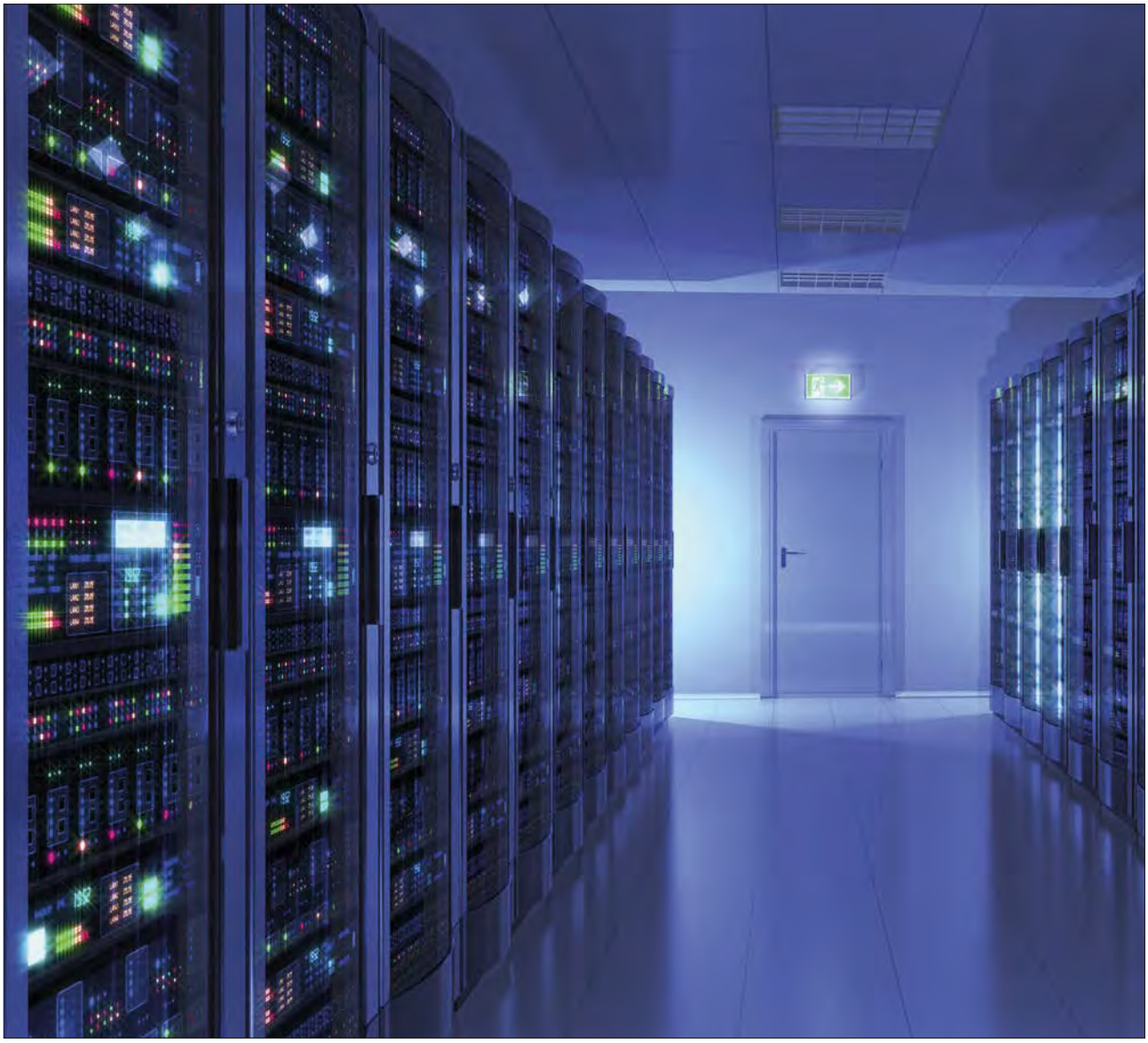
Operators of blockchains also have the burden of ensuring that their operations and the information shared on their ledgers are not in conflict with existing government regulations and data privacy laws.

Existing data privacy laws, such as those implemented by the Health Insurance Portability and Accountability Act (HIPAA) for example, also present hurdles for those developing distributed technology in the hopes of effectuating more efficient methods for the management of medical records or other sensitive material. Because the vast arena of existing privacy laws is too complex, and does not comport with the blockchain framework, adopting distributed technology for handling such data would necessarily imply dramatic changes to existing data privacy laws, or the creation of news ones.

While a blockchain's immutability was previously mentioned as an advantage, it may also come as a disadvantage in regard to the difficulty involved in correcting errors that were recorded, and the ledger's inability to reverse transactions. And while much of the appeal behind blockchain is its alleged efficiency, the Bank of Canada, after a year-long trial testing blockchain technology on interbank transactions between Canadian banks, declared that it will not be adopting "distributed ledger technology [because it] is unlikely to match the efficiency and net benefits of a centralized system." Canada's central bank went on to state that blockchain technology was not yet "safe, secure, and resilient" enough of a system to be implemented for interbank transactions.[10]

The size of a blockchain network is a function of the number of nodes running the network software and verifying transactions, known in the context of the Bitcoin blockchain as "miners." Bitcoin, for example, uses a proof-of-work mechanism to incentivize nodes to dedicate computer power to the network and thereby form the underlying hardware that maintains a full record of the distributed ledger and facilitates transactions. While smaller blockchain networks may offer more technical security options, they are not necessarily safer. Organizations that host blockchains that are open to outside participants to verify transactions should especially consider the possibility of so-called "51% attacks," where the majority of the network's hash rate, or processing power, is concentrated in a single node, thereby allowing that single node to manipulate the public ledger at will. The smaller the number of nodes on an open network, the higher the chances that hash rate can become concentrated. In addition, the pseudonymous nature of blockchain transactions can

4 the percentage of bitcoins that have been rendered permanently ownerless because users have misplaced their digital keys



make fraud detection and collusion between users more difficult to detect. Developers should carefully consider the sensitivity of information stored in a distributed ledger, the type and number of network participants, and the incentives for fair play on the network.

Open vs. closed blockchains

Blockchains can be developed in either an open distributed ledger or a closed one. An open or public distributed ledger is one that is available for anyone to use, and where users have the option to remain **anonymous** or **pseudo-anonymous** on that ledger. The Bitcoin blockchain is a model example of an open distributed ledger because anyone is allowed to access the ledger, mine bitcoins, and view the records of bitcoin transactions recorded on the ledger, without the need for revealing their identities. While an open blockchain guarantees transparency and accessibility—two major driving forces behind the growing popularity and approval for the use of distributed ledgers—unfettered access to an open blockchain by anyone could allow for security breaches of sensitive material and the feasibility of conducting illicit activity, such as the black market activity that tainted Bitcoin's initial reception. Open blockchains such as Bitcoin have also been known to perform significantly more slowly than closed ones, because of the high volumes of user traffic in those ledgers.

A closed or permissioned distributed ledger, on the other hand, is one that requires permission to gain access to, and where the identities of that ledger's users

are known, similar to a private computer or internet network. Developers of closed blockchains create them in a way that allows for restrictions on who may access, use, and validate transactions on the ledger. A closed blockchain's ability to allow for administrative control of its users while still retaining the efficiency and lowered transaction costs of a distributed ledger has attracted many industries, especially those dealing with private capital and sensitive records, such as banks and health care. Since the idea of having one's financial transactions, for example, being validated by an anonymous party can be unsettling for many, a closed blockchain accounting for the true identity of who exactly validates them can offer some network participants more peace of mind.

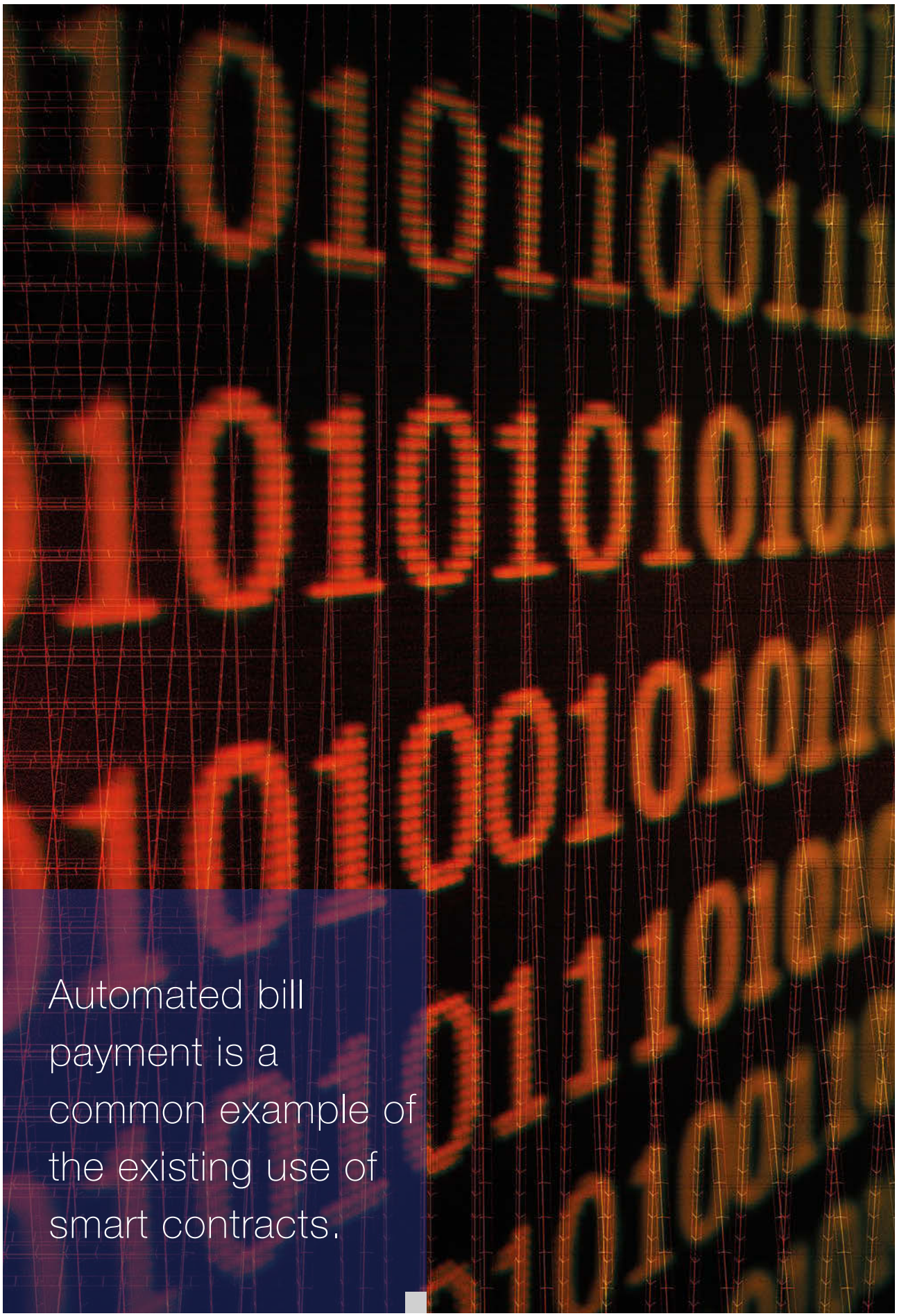
While permissioned blockchains have their obvious security benefits in terms of privacy, they are less de-centralized and thus less transparent. This has caused critics to view closed distributed ledgers as going against the purpose of creating distributed ledgers such as blockchain, some even refusing to acknowledge them as "true" blockchains. Fewer administrators would also mean fewer people needed to target and infiltrate a closed blockchain, raising important questions regarding their security.

Proof of work vs. proof of stake

One disadvantage of using proof of work to achieve consensus in a distributed ledger is the energy cost of the network's mining algorithm. As each mining node races to discover the next nonce to record a block (and claim the mining fee), more and more power is consumed by miners to achieve a competitive hash rate. An alternative incentive mechanism, proof of stake, avoids this problem by distributing mining fees in a pseudorandom manner based on the size and/or age of a miner's stake in the network. In other words, the more a miner holds in a proof of stake digital currency, the higher the chances he or she will obtain a mining fee when new blocks are recorded. This relieves the competitive computing power pressure that causes proof of work blockchains to consume excessive energy. Often, proof of work digital currencies, such as Dash, are treated as a passive investment, wherein the miner's stake gains "dividends" over time.[11] However, the proof of stake approach does not cure all. Criticisms include that relying on the quantity of a miner's stake means that it is possible to concentrate power in a small number of nodes, increasing the chances of tampering.

Summary

The blockchain algorithm is an important contribution to the foundational technologies we use to store and secure information. It addresses particular problems with counterparty trust and digital asset ownership. While not a panacea, the blockchain algorithm presents exciting opportunities in how we store and share information securely online. Many commentators posit that the invention of the blockchain will be remembered in the same vein as the invention of the World Wide Web or email. As a foundational technology, the blockchain could one day be a major part of how we store and transmit electronic information itself. The opportunity is wide open for innovators to apply blockchain across the digital landscape.


Automated bill payment is a common example of the existing use of smart contracts.

Smart contracts

What they are

Smart contracts are transactions that are automatically verified and executed through the use of computer software that translates contract terms into code. Unlike the typical offer and acceptance model of contract formation, smart contracts are integrated with an input/output structure based on a series of pre-determined if/then conditionals, where the encoded terms of an offer are accepted by the counterparty's performance. Under the smart contract framework, input code signifying that the terms of the offer have been met triggers output, the performance of the contract. "Smart" thus refers to the fact that some elements of the contracts are automatic and self-executing in accordance with pre-defined conditions. Individual provisions of an agreement, or entire agreements, can be converted into executable code and broadcast to nodes on a blockchain.

Smart contracts can receive data from oracles, allowing the on-chain contracts to interact with the off-chain world. An oracle is simply an independent third party or agent that controls data, such as pricing information or actuarial tables. The oracle allows the smart contract to query an off-chain data source to determine if a triggering event has occurred.

Automated bill payment is a common example of the existing use of smart contracts. In those transactions, the person paying can electronically "tell" computer software, designated by the person or entity receiving the payments, to timely and automatically charge their credit card the balance due. If it is the last day of the month, then X's credit card is charged. If X pays his cable bill for the month, then Y will allow his cable to stay on for a month. Inversely, if X does not pay his cable bill for the month, because he deleted his credit card information on Y's website or because of insufficient funds, for example, then Y can automatically disconnect his cable until he does so.

Smart contracts can be programmed and run as software on any network. By executing smart contracts on a blockchain, however, these if/then conditional variables are encoded into a neutral ledger that automatically triggers output once both parties' input conditions are met. In the above example, instead of X having to deposit funds into Y's account through Y's website, and then Y turning or keeping on X's cable, X's funds would be transferred to a blockchain where it would not be deposited into Y's account until Y continues X's cable.

Advantages of smart contracts on blockchains

Smart contracts executed on a distributed ledger, as opposed to on a centralized one, allow for equal footing and leverage to both parties involved in the transaction.

Smart contracts may be a natural fit to streamline enforcement of standardized derivatives contract terms, and facilitate compliance with new regulations.

Traditionally, contracts are drafted to be more favorable to the drafter. The terms of a smart contract are in code, and as such are less likely to be linguistically ambiguous. That is because if/then conditional computations require clearly defined inputs and outputs to function. And because computer software is gathering information from all parties to a transaction, the parties are less likely to breach smart contracts. Although legal issues will arise in some cases, such as when dealing with complex transactions, transacting through smart contracts significantly lowers the risk of breach.

Through a distributed ledger, a buyer and seller can conduct business without having to seek a trusted third party to ensure the contract's terms are honored. The ledger's immutable record ensures full transparency. This allows for the successful completion of paperless transactions without the need for a middle man such as a bank or a broker to facilitate or administer the contract's execution.

Conducting transactions by smart contracts on a blockchain is especially appealing to those in fields such as financial services. Smart contracts bypass the many cumbersome steps a transaction must go through in the clearing and settlement process. By having all the necessary "inputs" from those involved in the transaction sent to a distributed ledger, as opposed to individually clearing every step involved in the paper trail to a centralized ledger, a higher volume of transactions is efficiently completed, and at a faster rate. This also reduces transaction costs by cutting out fees associated with processing and third-party intermediaries. Creative industries can additionally benefit from smart contracts conducted on blockchain because blockchain enables seamless peer-to-peer transactions by buyers and sellers, allowing, for example, collectors to purchase or trade art without the need of a broker.

Disadvantages of smart contracts

Although the use of smart contracts on a blockchain could revolutionize transactions by dramatically increasing efficiency, cutting down transaction costs, and allowing for full transparency between parties, the smart contract framework itself is not a novel idea. As such, existing applications of smart contract technology operating without issue without the use of a distributed ledger raises the question of whether implementation on a blockchain would be a waste of time, energy, and resources.

One such example is "starter interrupter" technology that is used in certain car leases. This technology allows a car lessor or creditor to automatically and remotely prohibit the leased car from starting if the lessee has not made due payments or has breached any term of the lease agreement. Transferring the operation of this seemingly adequate technology to a distributed ledger would be a misguided attempt for increased efficiency and lower transaction costs, as the cost for implementing blockchain technology would likely not outweigh the benefits.

Another problem with smart contracts is the issue of legality. States and nation states have differing views on the legal standing of electronic signatures, smart contracts and blockchain technology, as discussed in more detail below. Many states provide little or no guidance on the subject and, thus, issues related to enforceability in differing jurisdictions are inevitable. For example, cross-border netting is complicated

even without adding automatic decentralized execution. Because no uniform procedure for inter-state and transnational smart contract execution currently exists, the process of transacting through cross-border smart contracts has the potential to be burdensome and tedious, taking away from the transactional efficiency smart contracts were designed to promote. In a globalized world with a market that is becoming progressively more inter-connected, key industries with high international transaction volume, such as finance, will have to tackle the hurdles of enforceability before reaping the benefits of smart contracts.

Smart contracts and derivatives

Payments and deliveries in derivatives trades are heavily dependent on conditional logic, and thus lend themselves more readily to automation than other transactions. Smart contracts may be a natural fit to streamline enforcement of standardized derivatives contract terms, and facilitate compliance with new regulations.

To further the commitments made at the 2009 G20 summit in Pittsburgh, regulators throughout the world have promulgated clearing, margining, trade execution, reporting, and other compliance requirements for over-the-counter derivative transactions. In the face of these new complexities, the International Swaps and Derivatives Association (**ISDA**) and others have opined that smart contracts could (and perhaps should) play a key role in the development of a standardized, efficient, and compliant marketplace. ISDA proposes the use of a blockchain to store electronic ISDA Master Agreements. The agreements would contain conditional logic triggers programmed by smart contract code, which would facilitate the automation of certain provisions within swaps documentation. Day-to-day compliance with the regulations could be embedded into smart contracts. For example, bank accounts or digital currency wallets could be linked to the smart contract and automatically exchange variation margin as required. Similarly, the smart contract could be designed to automatically submit data and reports to trade data repositories upon the occurrence of a triggering event.

Some financial institutions are already experimenting with smart contracts and derivatives. Barclays recently tested R3's Corda platform to execute swaps using smart contracts.[12] DTCC and six other firms similarly tested blockchain technology that uses smart contracts to manage post-trade lifecycle events for credit default swaps.[13] We expect to see more smart contract implementation in financial markets in the near future.

digital assets have become the target of regulations issued by federal and state agencies.

U.S. regulatory landscape

In the United States, it is currently legal to transmit, mine, and develop "virtual currencies,"[14] such as bitcoin and ether. It is also generally legal to purchase goods and services with these instruments, or to buy and sell them as investments. Finally, it is also generally legal to use and/or develop virtual currency technology and software, including multi-signature wallets, and to utilize blockchain and distributed ledger technology for both monetary and non-monetary purposes (for example, smart property and smart contracts).

However, with their dramatic increase in prevalence and overall use, virtual currencies have become the target of regulations issued by federal and state agencies. The increase in regulatory oversight has been particularly significant during the past two years.

The state of New York has already issued regulations explicitly subjecting those engaging in virtual currency-based business activities to licensing, supervision, and other compliance requirements.

In addition, various federal agencies have clarified through guidance that certain virtual currency-related activities may be subject to already-existing regulations, such as those governing money transmission. In addition, in a move that could impact all types of FinTech firms—including virtual currency companies—the Office of the Comptroller of the Currency has announced a proposed framework under which the OCC would grant a special purpose national bank charter to FinTech companies. Furthermore, several agencies have initiated enforcement actions against businesses and individuals related to virtual currency activities.

The focus of these regulations tends to be on the virtual currencies themselves and their transmission, as opposed to the pure development of blockchain technology and software. For example, the New York BitLicense regulations explicitly provide that those who only develop blockchain software and technology are not subject to licensure. In addition, states such as North Carolina and Illinois have specifically excluded the development and provision of multi-signature software and use of distributed ledger technology for non-monetary purposes from the states' respective money transmission statutes.

NYDFS has denied five BitLicense applications and ordered the companies receiving denial letters to stop any operations in New York.

These recently promulgated regulatory regimes, along with the guidance provided by other agencies clarifying the application of already existing regulations to virtual currency-related activities, have major implications for companies engaged in virtual currency activities from a licensing, supervision, compliance, and cost perspective. Undoubtedly, with the sustained growth of virtual currencies, governments will continue to adapt, and one can expect additional regulations from governmental authorities within the coming years.

State regulation

New York: the BitLicense regime

New York State has been at the forefront of virtual currency regulation since 2014. In July 2014, through its Department of Financial Services (NYDFS), New York became the first state to propose a comprehensive regulatory regime governing virtual currency business activities.[15] And on June 3, 2015, following comments from numerous interested parties, New York became the first state to implement a comprehensive virtual currency regulatory regime – popularly known as "BitLicense."[16]

As of June 2016, NYDFS has received 26 initial BitLicense applications.[17] Yet, as of October 2017, NYDFS has issued only three licenses under the BitLicense regime.[18] NYDFS has denied five BitLicense applications and ordered the companies receiving denial letters to stop any operations in New York.[19] NYDFS issued its first license in September 2015 to Circle Internet Financial, a bitcoin wallet and creator of the app Circle Pay that was backed by multiple investors, including Goldman Sachs, IDG Capital, and Baidu.[20] The agency issued its second license in June 2016, to XRP II, LLC, an affiliate of Ripple.[21] And NYDFS issued its most recent license—in January 2017—to Coinbase, Inc.[22] NYDFS has also granted charters under the New York Banking Law to Gemini Trust Company and itBit Trust Company as virtual currency firms acting as trust companies.[23]

Under the BitLicense regime, companies engaged in "virtual currency business activities" are required to undergo a thorough application process, obtain a license, abide by numerous compliance requirements similar to banks and other financial institutions, and be subject to examinations by NYDFS.

The BitLicense regulations are controversial, and some have criticized the burdens that they place on virtual currency-related businesses. Companies are faced with a stark choice: apply for a license that has only been granted to a select few companies and imposes burdensome compliance obligations on the licensee, or avoid doing business in the state of New York altogether. As a result, some companies have attempted to block users in New York from using their technology in an attempt to avoid falling under the BitLicense regulations.[24]

Who must obtain a license?

Under BitLicense, a "virtual currency" is a digital unit that is a digital medium of exchange or form of stored value, with specific exceptions for prepaid cards, customer rewards programs, in-game currency and reward points.[25]

Companies that conduct "virtual currency business activities," as defined in the BitLicense regulations, and

that operate in New York, or engage in business with New York customers, are subject to the BitLicense regime.[26]

Under BitLicense, the following five activities constitute "virtual currency business activities":

- **Receiving** virtual currency **for transmission, or transmitting** virtual currency through a third party
- **Maintaining custody** of virtual currency or holding virtual currency on behalf of others
- **Buying or selling** virtual currency **as a customer business**
- Performing virtual currency **exchange or conversion services** (whether converting virtual currency to fiat currency or vice versa; or converting one type of virtual currency for another type of virtual currency)
- **Controlling, administering, or issuing virtual currency**[27]

BitLicense exempts several activities from licensure. For example, virtual-currency mining on its own would not subject a party to the BitLicense regime.[28] Similarly, consumers or merchants only using virtual currency to buy or sell goods or services would not be required to obtain a license.[29] And finally, parties who engage purely in software development and dissemination do not fall under BitLicense.[30] However, there are many unanswered questions as to the particular circumstances in which various exceptions would apply. For example, BitLicense exempts from licensure the transmission of "nominal amounts" of virtual currency for "non-financial purposes."[31] Some have surmised that this would allow for transmission of nominal amounts of virtual currency for purposes of, for example, identity verification. However, whether this exception would apply to the use of a nominal amount of virtual currency to create a "digital contract" is less clear. Likewise, there are several gray areas as to whether certain businesses are engaged in one of the five "virtual currency business activities," or in mere software development.

Application and licensing process

The BitLicense application and licensing process is extensive, and is similar to the licensing required for other types of financial institutions chartered in New York. Applicants must pay a $5,000 application fee, and submit to NYDFS extensive biographical, historical, financial, and business information about the applicant, its principal officers, and its principal stockholders.[32] Under BitLicense, NYDFS must approve or deny applications within 90 days of deeming the application complete.[33] However, in practice, the regulators can also ask for more documentation, and likely often will, as is the case with other financial regulatory licensing. Further, the superintendent may also extend the 90-day window in certain cases.[34] Therefore, as with the licensing process for other financial institutions, the BitLicense application appears onerous and very time- and cost-intensive.

NYDFS may also issue conditional licenses under BitLicense for those applicants that do not comply with all BitLicense requirements upon licensing.[35] This conditional license is valid for two years. However, the conditional license may be issued subject to reasonable conditions imposed by NYDFS, and the licensee may be subject to heightened scrutiny, review, and examination.

the BitLicense application appears onerous and very time- and cost-intensive.

Licensees must also obtain NYDFS written approval to offer any materially new product, service, or activity, or to make a material change to an existing product, service, or activity.[36] Finally, NYDFS has the authority to suspend or revoke both full and conditional licenses on several grounds, including on any ground that the superintendent may refuse an initial license, for violation of any provision of BitLicense, good cause, or for failure to pay a judgment.[37]

AML, KYC, compliance issues, and examinations

Perhaps the most significant BitLicense provisions are the numerous ongoing compliance provisions that the NYDFS requires of licensees. Many such compliance regulations are similar to those required of New York-chartered banks and other types of financial institutions.

Licensees under BitLicense must maintain a comprehensive anti-money laundering ("AML") policy.[38] This policy is subject to both an initial risk assessment and ongoing annual risk assessments.[39] Licensees must adopt internal controls and policies to ensure AML compliance, including appointing a dedicated compliance officer, and subjecting the policy to review and approval by the licensee's board of directors.[40] The policy must be subject to annual independent testing, and the audit report must be submitted to NYDFS.[41]

The AML provisions also include numerous additional know-your-customer ("KYC") requirements similar to those in existence for other financial institutions, or for money transmitters under FinCEN regulations.[42] Licensees must identify and verify customers' identities, check customers against the list of Specifically Designated Nationals maintained by the Office of Foreign Assets Control (OFAC), and maintain customer records.[43] Licensees are also required to submit to NYDFS suspicious activity reports (SARs), and currency transaction reports for transactions in virtual currency of more than $10,000.[44]

Additional compliance regulations promulgated by the BitLicense regime include those addressing a licensee's:

Licensees are also required to submit to NYDFS suspicious activity reports (SARs), and currency transaction reports for transactions in digital currency of more than

$10,000

- Capital requirements[40]
- Custody and protection of assets[41]
- Books and records[42]
- Consumer protection disclosures[43]
- Consumer complaint policies[44]
- Advertising[45]
- Anti-fraud policies[46]
- Cybersecurity programs[47]
- Business continuity and disaster recovery plans[48]

Under BitLicense, licensees are subject to at least one examination by NYDFS every two years.[54] Licensees must also submit numerous financial statements and reports to NYDFS on a quarterly and annual basis.[55]

Other state virtual currency statutes

Several other states have enacted statutes governing virtual currency. Although these statutes do not create a comprehensive virtual currency regulatory regime in the style of New York's BitLicense, the statutes do add clarity to the treatment of virtual currency businesses under state money transmission law.

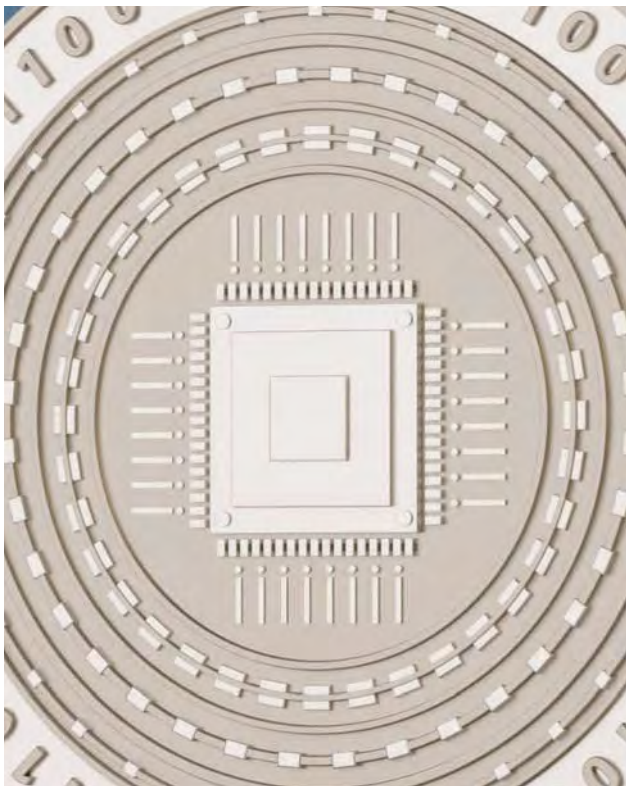
On June 19, 2015, shortly after enactment of New York's BitLicense regime, Connecticut Gov. Dannel

Malloy signed into law Substitute House Bill Number 6800. The law amended Connecticut's Money Transmission Act to define "virtual currency," and to specifically subject businesses engaging in transmission of virtual currency to the Act, including its licensure requirement.[56] However, the revised Act also subjects virtual currency businesses to additional requirements not applicable to transmitters of traditional currency. Specifically, all applicants must specify whether they intend to transmit monetary value in the form of virtual currency; virtual currency transmitters are subject to separate, individualized bond requirements determined by the Connecticut Banking Commissioner; the Commissioner is granted wide latitude in placing additional conditions or requirements on licensure of virtual currency transmitters; and the Commissioner may deny an application to engage in virtual currency transmission "if, in the commissioner's discretion, the issuance of such a license would represent undue risk of financial loss to consumers, considering the applicant's proposed business model."[57]

In January 2016, New Hampshire's Licensing of Money Transmitters statute was amended to specifically cover transmitters of virtual currency. Under that statute, any person engaging in money transmission, which included "[r]eceiving currency or monetary value for transmission to another location," must obtain a license.[58] The definition of "monetary value" was amended to specifically include "convertible virtual currency."[59]

However, the reaction to that legislation by virtual currency advocates and some New Hampshire legislators was swift and largely negative. In response, New Hampshire legislators introduced House Bill 436, which was signed into law June 2, 2017, and significantly deregulates virtual currency activity in the state. Most significantly, HB 436 exempts from the Money Transmitters statute "persons conducting business using transactions conducted in whole or in part in virtual currency."[60] And while some state regulators have issued guidance clarifying that they do not view a transaction involving the transmission of solely virtual currency as falling under their state's money transmission statute (see below), New Hampshire's HB 436 appears to go even further by exempting transactions conducted "in whole or in part in virtual currency." The bill also broadens the definition of "money transmission" to include "maintaining control of virtual currency on behalf of others."[61]

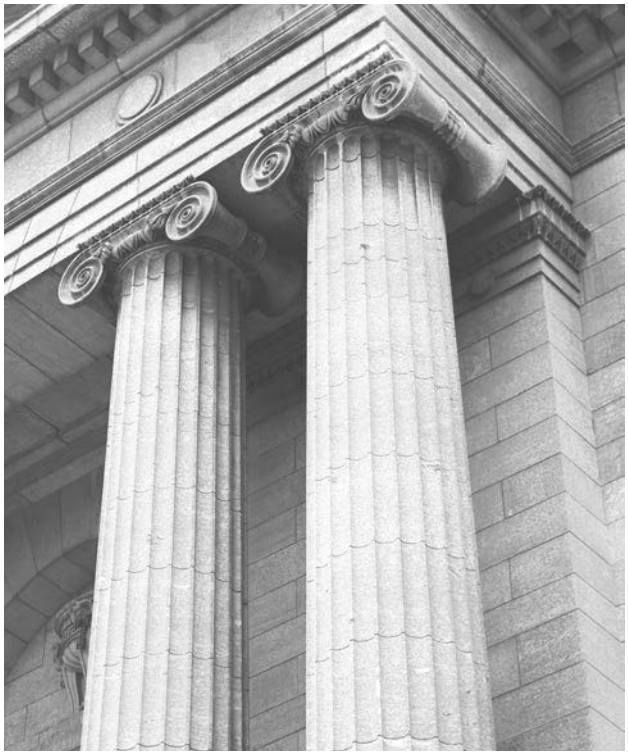
In July 2016, North Carolina's revised Money Transmitters Act was signed into law. The revised



Act clarifies the state's treatment of virtual currency businesses from a money transmission standpoint by specifically defining "virtual currency" as a "digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account, or a store of value . . . but does not have legal tender status as recognized by the United States Government."[62] The Act also specifically defines "money transmission" as including "maintaining control of virtual currency on behalf of others."[63] Therefore, virtual currency businesses engaging in such activities in North Carolina would

require a state money transmitter license. However, unlike Connecticut, transmitters of virtual currency would not be subjected to any different requirements than transmitters of traditional currency. The revised Act codified, in part, guidance issued in December 2015 by the North Carolina Commissioner of Banks concerning state treatment of virtual currency activities. In this guidance, the Commissioner clarified that virtual currency mining, the use of virtual currency, virtual currency administration, providers of multi-signature software, and blockchain 2.0 technologies generally, are not governed under the Money Transmitters Act and do not require licensure.[64] The revised Act and the Commissioner's guidance was generally supported by industry players, especially compared with New York's BitLicense. For example, Perianne Boring of the Chamber of Digital Commerce described the Act as "a business-friendly bill" that "gives better guidance to businesses," and "adds more clarity than any other state by a long shot."[65]

In April 2017, Washington State signed Senate Bill 5031, placing all operators of virtual currency under the jurisdiction of Washington State's money transmitter laws.[66] The bill, which took effect July 23, 2017, requires all operators of virtual currency to comply with the licensing and bond requirements imposed on all other money transmitters by the time the bill goes into effect. Senate Bill 5031 also introduces additional requirements specific to transmitters of virtual currency, including third-party audits, trade name rules and restrictions, and mandatory client disclosures.



At least five states so far have issued guidance as to how their state's law, particularly statutes and regulations concerning money transmission, applies to virtual currency transactions. Even prior to the official amendment of the state's Uniform Money Services Act, Washington state's Department of Financial Institutions concluded in agency guidance that virtual currency was included in the definition of "money transmission" in the Act, and therefore a company engaging in the business of offering virtual currency transmission services, or the ability to exchange virtual currency for another type of virtual currency, was required to register with the state as a money transmitter.[67] However, Kansas, Texas, Tennessee and Illinois have concluded that virtual currency does not constitute money under its money transmission laws, and therefore, the states' respective money transmission laws generally do not apply to virtual currency transactions. One potential exception in which all four states' money transmission laws may apply is a transaction in which virtual currency is exchanged for sovereign fiat currency through a third-party exchange site.[68] The guidance from the Illinois Department of Financial and Professional Regulation (IDFPR) also explicitly provides that virtual currency mining, use or development of multi-signature software, and use of a virtual currency's blockchain or distributed ledger technology for non-monetary purposes (including smart property and smart contracts), would not be considered money transmission under the Illinois Transmitters of Money Act.[69]

The Hawaii Department of Financial Institutions has not issued any formal regulatory guidance on virtual currency. However, the Department has privately informed at least one virtual currency company—

Coinbase—that companies offering virtual currency services in Hawaii will be required to obtain a license under the state's Money Transmission statute.[70] Perhaps more significantly, the Department also informed Coinbase that virtual currency would not be considered a "permissible investment" under the statute.[71] This stands in contrast to North Carolina and, more recently, Vermont's money transmission statute, which was amended May 1, 2017, to similarly include virtual currency owned by the licensee as permissible investments, but only to the extent of outstanding transmission obligations received by the licensee.[72] The practical effect of the Department's position is that companies holding virtual currency on behalf of customers would be required to hold additional fiat currency reserves in an amount equal to the amount of virtual currency held.[73] This position caused Coinbase to suspend its operations in Hawaii as of February 2017, because the company concluded it would be "impractical, costly, and inefficient for us to establish a redundant reserve of fiat currency over and above customer digital currency secured on our platform."[74]

Similarly, the Wisconsin Department of Financial Institutions has not issued any formal regulations or guidance as to the application of virtual currency to the state's Sellers of Checks statute (governing money transmission). Nevertheless, the Department's website states that "[t]he division is unwilling, at this time, to license companies to transmit virtual currency."[75] In June 2015, the Department entered into agreements with two virtual currency companies that had previously obtained Sellers of Checks licenses—CoinX Inc. and Circle Internet Financial Inc.—pursuant to which the companies agreed to only engage in transmission of fiat currency under their Wisconsin licenses.[76]

Finally, although not issued by a state regulator, a Florida state trial judge based in Miami ruled in July 2016 that Bitcoin was not "money" for purposes of Florida's money transmission statute.[77] In dismissing criminal charges against Michell Espinoza for unlawfully engaging as an unlicensed money transmitter and for money laundering, Judge Teresa Pooler wrote that, while the "Florida legislature may choose to adopt statutes regulating virtual currency in the future," based on the current money transmission statute, "attempting to fit the sale of Bitcoin into a statutory scheme regulating money services businesses is like fitting a square peg in a round hole."[78]

Conference of State Bank Supervisors

On September 15, 2015, the Conference of State Bank Supervisors issued a model licensing regime as a guide to states in regulating virtual currency. The Conference recommends that companies involved in the exchange and transmission of virtual currencies and "services that facilitate the third-party exchange, storage and/or transmission of virtual currency (e.g. wallets, vaults, kiosks, merchant-acquirers, and payment processors)," be supervised and licensed by state banking regulators.[79] "Virtual currency" is defined here as a digital representation of value used as a medium of exchange, unit of account, or store of value, but which does not hold legal tender status. Virtual currency would not include the software or protocols governing transfer.[80]

Other state proposals

Following New York's lead, other states have made various proposals to implement virtual currency regulations over the past several years.

Perhaps most prominently, in June 2015, the California House of Representatives passed AB-1326.[81] The bill, introduced in February 2015, would provide for a similar, but not quite as extensive, licensing regime to New York's BitLicense.[82] Like BitLicense, AB-1326 would provide that virtual currency businesses could not operate unless licensed by the California Department of Business Oversight. The proposal also calls for capital requirements and an extensive application process. However, the California proposal would be more relaxed than BitLicense in certain areas: for example, it would not require submission of state-level SARs and would contain less stringent AML requirements. AB-1326 stalled in the California Senate in September 2015; a

revised version of the bill was revived in August 2016, but its sponsor pulled the bill shortly thereafter in the wake of opposition from various groups.[83] The bill is no longer listed as active; however, it could be revived on a future date.

Other states, including New Jersey, North Dakota, Pennsylvania, and Utah, have also made various virtual currency regulation proposals; however, none has been adopted as of this writing.[84]

State blockchain statutes

In March 2017, Arizona passed House Bill 2417 granting smart contracts and any blockchain-backed e-signatures or records binding legal status by placing them within the scope of the state's Electronic Transactions Act.[85] Similarly, Nevada passed Senate Bill 298 on June 5, 2017, stating that the "writing" requirement of a document can be legally satisfied under Nevada's UETA (Uniform Electronic Transactions Act) if the document is recorded on a blockchain and also bars the state's governments from imposing fees or licensing requirements on those using blockchain technology.[86] The legislation passed in Arizona and Nevada represents a shift in focus from the typical blockchain-related state legislation prevalent in other states, since they appear to be more concerned with regulating contract enforceability as opposed to the issues surrounding the regulation of money transmitters and virtual currency. Arizona and Nevada's bills also indicate that states considering passing laws concerning blockchain and smart contracts can do so by grouping them with existing state laws. But only a few weeks after signing House Bill 2417 into law, Arizona passed House Bill 2216 prohibiting the use of blockchain technology to "locate or control the use of a firearm" by non-law enforcement officers and a few other exempt individuals.[87]

In other states, many non-restrictive, blockchain-related legislative measures have been proposed and adopted. In June 2017, Vermont's governor signed S.135 into law, which would promote the use of blockchain technology throughout the state and conduct a study on the blockchain's risks and benefits in order "to promot[e]" economic development."[88] Similarly, Hawaii's House Bill 1481, introduced in the following month, proposes establishing a work study group to "determine best practices regarding blockchain technology."[89]

In June 2017, Illinois passed House Resolution 120, which formed a "Legislative Blockchain and Distributed Ledger Task Force" to study how the state government can benefit from a transition into a blockchain-based system of governmental record keeping.[90] Beyond the passage of HR 120, the Illinois state government has pursued an ambitious blockchain agenda through its Illinois Blockchain Initiative. Through the Initiative, the state, the IDPFR, other state agencies, and local governments are exploring ways to explore innovations involving blockchain technology and its potential impact on government. These efforts have included partnerships, collaborations, and pilot programs with various technology companies seeking to utilize blockchain technology to improve the efficiency and accuracy of, among other things, birth registration, land records, medical credentialing, financial markets.[91]

Federal regulation and guidance

Unlike New York State, federal agencies have not yet issued sets of regulations specifically addressing digital assets and virtual currency. However, in recent years, agencies have clarified that certain laws and regulations already in existence may apply to activities and transactions involving digital assets.

Commodity Futures Trading Commission (CFTC)

On September 17, 2015, the CFTC confirmed that it would treat bitcoin and other virtual currencies as "commodities" for regulatory purposes under the Commodity Exchange Act (CEA) and CFTC regulations.[92] Under the CEA and its regulations, the CFTC has jurisdiction over the trading of futures, options, and swaps on "commodities."[93] The term

"commodity" is defined broadly to include "goods and articles…and all services, rights and interests…"[94] The CFTC's operation of jurisdiction over virtual currency came in the form of a settlement order against Coinflip, Inc., which is discussed in more detail below. The decision to treat virtual currencies as "commodities" under the CEA and CFTC regulations confirms prior informal guidance provided by former CFTC Chairman Timothy Massad and other CFTC officials, who had commented in testimony and speeches that the CFTC would be able to assert jurisdiction over virtual currencies.[95] The order also appears to confirm that the CFTC would only treat virtual currency as a "commodity," and that it would not treat virtual currency as "currency"; and therefore, virtual currencies would not be subject to certain regulations governing foreign exchange derivatives.[96] The treatment of virtual currency as a "commodity" carries significant implications for businesses that engage in trading virtual currency-based derivatives. Such firms that come under the CFTC's jurisdiction may have to register with the CFTC, and could be subject to regulation by the CFTC and/or the National Futures Association. This supervision will undoubtedly subject the firms to numerous regulatory obligations. As a result of the CFTC's September 2015 settlement with Coinflip, almost any business whose business activities involve virtual currency-based derivatives will need to assess whether it is required to register with the CFTC and may be subject to CFTC regulation. Two such businesses might include firms running trading platforms involving virtual currency-based derivatives, or firms providing advisory services concerning virtual currency-based derivatives. Under the enforcement section below, we detail the follow-up actions the CFTC has brought against other virtual asset companies.

In 2017, the CFTC granted the virtual currency trading platform LedgerX registration as both a derivatives clearing organization (DCO) and a swap execution facility (SEF) under the CEA.[97] LedgerX, which launched in October 2017, is the first federally regulated virtual currency options exchange and clearinghouse in the United States. Additionally, the Chicago Mercantile Exchange and CBOE Futures Exchange self-certified futures contracts on bitcoin with the CFTC and launched the contracts in December 2017.[98]

The CFTC launched LabCFTC, a FinTech initiative that seeks to foster responsible innovation, in 2017.[99] LabCFTC works with FinTech companies to assist them in understanding how the U.S. commodities laws and regulations might affect their business.

Financial Crimes Enforcement Network (FinCEN)

Like the CFTC, **FinCEN** has not issued any regulations directly addressing virtual currency. However, businesses engaged in virtual currency activities may come under the purview of FinCEN's regulations concerning money services businesses (MSBs). Under FinCEN regulations, MSBs include "money transmitters."[100] In 2011, FinCEN opened the door to regulation of virtual currency businesses as money transmitters—and therefore MSBs—when it revised the definition of "money transmission services" to include "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[101] Therefore, any party that engages in the transmission of virtual currency must abide by FinCEN's MSB regulations, just as if the business transmitted traditional currency.

The implications for being deemed a money transmitter and MSB are significant. MSBs must comply with numerous AML requirements, including implementation, adoption, and maintenance of an AML program; independent review of such AML program; filing of SARs and currency transaction reports; and maintenance of records.[102] Further, MSBs must register with FinCEN. It is a federal crime to knowingly conduct an MSB while failing to register with FinCEN (or state licensing money transmission licensing agencies).[103]

Starting in 2013, FinCEN has issued guidance clarifying what types of virtual currency activities could

trigger treatment as an MSB by FinCEN. In March 2013, FinCEN provided three types of parties that may engage in virtual currency activities:

- **Users** (those who use virtual currency to purchase goods or services);
- **Exchangers** (those providing for the exchange of virtual currency for real currency, funds or other virtual currency);
- **Administrators** (those issuing virtual currency, or with the authority to redeem virtual currency).[104]
- FinCEN concluded that, broadly speaking, users of virtual currency would not be considered MSBs, but that exchangers and administrators **would** fall under the MSB regulations.[105]

Since then, FinCEN has provided additional guidance as to what types of activities may trigger regulation. FinCEN has issued various guidance providing that it would not view the following activities as subjecting a party to MSB regulations:

- Mining virtual currency;[106]
- Use of virtual currency to purchase goods and services;[107]
- Conversion of virtual currency to fiat currency for one's own use;[108]
- Investing in virtual currency for one's own account;[109]
- Renting out of computer systems and software that mine virtual currency to third parties (where any vitual currency mined by the third party using the software would remain the property of that third party).[110]
- Many of the above were deemed not to constitute the activities of an MSB because they were performed for one's own account; however, as soon as such activities were performed by or on behalf of a third party, the analysis could change.
- On the other hand, FinCEN has confirmed that the following activities would constitute engaging in business as an MSB:
- Maintaining a trading system to match offers to buy and sell virtual currency for fiat currency;[111]
- Maintaining a set of book accounts where customers may deposit virtual currency;[112]
- Developing and maintaining a system to provide virtual currency payments to merchants in the United States and Latin America wishing to receive payment for goods/services sold in a currency other than that of legal tender;[113]
- Conducting Internet-based brokerage services between buyers and sellers of precious metals, in which buyers pay sellers directly by check, wire, or bitcoin; and the entity uses the bitcoin blockchain to transfer previous metal ownership by issuing a digital certificate. The customer could then later exchange its holdings using the bitcoin blockchain ledger.[114]

It is a federal crime to knowingly conduct an MSB while failing to register with FinCEN

Office of the Comptroller of the Currency (OCC)

In December 2016, the OCC announced it would consider granting FinTech firms special purpose national bank charters.[115] Although these charters would be aimed more broadly at the FinTech industry—and not only at virtual currency firms—the impact of the charters on virtual currency regulation could be significant. The OCC argues that such a charter framework

would promote the safety and soundness of FinTech institutions.

Under the OCC's proposed framework, FinTech companies could apply for a special purpose national bank charter, similar to the type of charter that the OCC has granted to trust banks and credit card banks. In order to apply for the special purpose charter, a FinTech company would be required to either engage in fiduciary activities, or perform at least one of three types of banking services—receiving deposits, paying checks, or lending money.[116] However, the OCC has argued that these banking services may be construed broadly, noting in particular that companies "engaging in … means of facilitating payments electronically" could apply for charters because such services "are the modern equivalent of paying checks."[117]

Under the proposal, FinTech companies that apply for a special purpose charter would be treated similarly to national banks from the standpoint of both charter application and approval, and subsequent ongoing regulation. In March 2017, the OCC released a draft licensing manual supplement explaining the licensing process, as well as the factors it would consider in determining whether to grant a special purpose charter to FinTech companies.[118] As is the case with national banks, the OCC would encourage applicants to arrange a pre-filing meeting with the OCC to discuss an upcoming application.[119] Applicants would be required to submit a robust business plan, and the OCC would carefully evaluate the company's capital, liquidity, compliance, and governance structure.[120]

After receiving a special purpose charter, FinTech firms would be subject to the OCC's regulatory scrutiny, and the OCC has indicated it would hold such companies to rigorous standards on issues concerning safety and soundness, capital requirements, anti-money laundering, financial inclusion and consumer protection.[121] Although the regulatory and compliance burdens for FinTech firms with a special purpose charter would undoubtedly be high, the FinTech companies would benefit because they would be governed by a single national regulator, and would only be required to obtain a single charter from a national regulator, as opposed to licenses across all states. Further, because OCC regulations would generally preempt state laws (as is the case for national banks), FinTech charter recipients could follow a single, uniform set of regulations, as opposed to 50 sets of state regulations that may be inconsistent and difficult to track.

The OCC's proposal was generally greeted positively by FinTech companies, who argue that the current U.S. regulatory structure hurts innovation, and that the proposed framework will reduce regulatory complexity and allow companies to more easily operate nationwide.[122] This could be especially relevant for virtual currency firms, because such companies often seek to operate on a nationwide basis, and because the regulations impacting virtual currency companies and services on a state-by-state basis are still uncertain and developing.

However, state regulators have opposed the framework, arguing that states are the best regulators of non-banking financial services companies and best ensure consumer protection. The NYDFS issued a particularly critical letter to the OCC opposing the proposed special purpose charter, arguing that the "imposition of an entirely new federal regulatory scheme on an already fully functional and deeply rooted state regulatory landscape will invite serious risk of regulatory confusion and uncertainty, stifle small business innovation, create institutions that are too big to fail, imperil crucially important state-based consumer protection laws and increase the risks presented by nonbank entities."[123] And on April 26, 2017, in perhaps the most direct threat to the OCC's FinTech charter, the Conference of State Bank Supervisors (CSBS) brought suit against the OCC in federal district court, arguing that, in promulgating the special purpose FinTech charter, the OCC exceeded its statutory authority under the National Bank Act and violated the Administrative Procedure Act.[124] Less than three weeks later, on May 12, 2017, the NYDFS followed up by filing a suit of its own in federal district court against the OCC; the suit raised similar issues and brought similar causes of action as the CSBS suit.[125]

Securities and Exchange Commission (SEC)

Until recently, the SEC had taken a backseat and allowed other regulators to police the crypto asset markets. 2017 marked a sea change for the agency. In 2017, the SEC rejected two bitcoin-backed exchange-traded funds (ETF), released an investigation report related to an initial coin offering (ICO), and suspended trading in company securities of three blockchain-related companies.

In March 2017, the SEC rejected two separate bids to list bitcoin-backed ETFs, which would only hold bitcoins as assets. On March 10, 2017, the SEC rejected an application for the Winklevoss Bitcoin Trust to be listed on the Bats BZX Exchange—one of the largest ETF exchanges.[126] The SEC rejected the application because it was not confident such an ETF would "be designed to prevent fraudulent and manipulative acts and practices and to protect investors and the public interest."[127] Further, exchanges that list commodity-trust exchange-traded products "must have surveillance-sharing agreements with significant markets for trading the underlying commodity . . . [and] those markets must be regulated."[128] However, the SEC found "that the significant markets for bitcoin are unregulated," and "the exchange would therefore be unable to enter into "the type of surveillance-sharing agreement that has been in place with respect to all previously approved commodity-trust ETFs—agreements that help address concerns about the potential for fraudulent or manipulative acts and practices in this market."[129] However, the SEC did note that "bitcoin is still in the relatively early stages of its development and that, over time, regulated bitcoin-related markets of significant size may develop."[130] On March 28, 2017, the SEC also rejected an application to list the SolidX Bitcoin Trust ETF on the New York Stock Exchange for similar reasons.[131] However, on April 24, 2017, the SEC announced it would review its decision to reject the WInklevoss Bitcoin Trust, potentially giving bitcoin-ETFs a second chance.[132]

Each of these SEC decisions has had a significant impact on the price of bitcoin. On March 3, 2017, prior to the SEC's decision on the WInklevoss Trust, when many investors anticipated a favorable outcome, the price of bitcoin hit a record high; following the rejection on March 10, the price tumbled by 18 percent; and following the SEC's decision to reconsider its rejection of the Winklevoss Trust, bitcoin rebounded to hit another near high.[133]

On July 25, 2017, the SEC issued an **Investigative Report** detailing its investigation of an ICO of crypto tokens representing interests in "The DAO," a decentralized autonomous organization, through the Ethereum blockchain.[134] The SEC also released a related Investor Bulletin on ICOs, and warned that some crypto "tokens" or "coins" may qualify as "securities" subject to the SEC's jurisdiction that must be offered and exchanged in compliance with the securities laws and regulations. The SEC places this subset of crypto assets within the catchall category of securities known as "investment contracts," and will use the facts-and-circumstances test set forth in SEC v. Howey to determine whether a given product must be offered in conformity with the federal securities laws.

Shortly after issuing The DAO report, in August 2017, the SEC suspended trading in the company securities of three blockchain-related businesses. On August 9, 2017, the SEC issued an order suspending trading in the securities of CIAO Group, Inc. because of questions regarding the accuracy of statements in its press releases pertaining to, among other things, plans for an ICO.[135] On August 23, 2017, the SEC issued an order suspending trading in the securities of First Bitcoin Capital Corp., a Canadian company that has issued seven crypto tokens, because of concerns regarding the accuracy and adequacy of publicly available information about the company, including the value of its assets and capital structure.[136] However, the SEC did not suspend trading in any of the company's crypto tokens. On August 28, 2017, the SEC suspended trading in the securities of American Security Resources Corp., which intends to launch a digital currency exchange, due to questions regarding information included in press

releases about the company's business transition to the crypto asset markets, and adoption of blockchain technology.[137]

The SEC recently announced the establishment of a Cyber Unit and retail strategy task force to better enable its Division of Enforcement to address cyber-based threats and protect retail investors.[138] One area of the Cyber Unit's stated focus will be potential violations involving distributed ledger technology and initial coin offerings (ICOs).

Internal Revenue Service (IRS)

The Internal Revenue Service has concluded that digital currency should be considered "property" under the Internal Revenue Code, and thus transfers involving virtual currencies would be taxable events.[139] However, the IRS was criticized by its own internal inspector general in September 2016 for failing to implement this guidance in practice, finding "there has been little evidence of coordination between the responsible functions to identify and address, on a program level, potential taxpayer noncompliance issues for transactions involving virtual currency."[140] Perhaps not coincidentally, the IRS appears to have become more aggressive in recent months in attempting to enforce potential tax violations involving virtual currency transactions. Two months after issuance of the report, the IRS sought authority in federal court to issue a "John Doe" summons on Coinbase for the purpose of determining the identities of all U.S. Coinbase customers who engaged in virtual currency transactions in 2013 and 2014.[141] Under federal law, the IRS may only issue such a "John Doe" summons if it can establish that there "is a reasonable basis for believing that such person or group or class of persons may fail or may have failed to comply with any provision of any internal revenue law."[142]

Financial Industry Regulatory Authority (FINRA)

In January 2017, FINRA issued a detailed report on Distributed Ledger Technology: Implications of Blockchain for the Securities Industry. Although FINRA has not issued any digital currency-specific regulations or rules of its own, the report does caution broker-dealers that may wish to become more involved with digital currency and distributed ledger technology, to be cognizant of various SEC and FINRA rules that may impact digital currency transactions. This could include rules concerning customer funds and securities, net capital, books and records, clearance and settlement, AML and KYC programs, data privacy, trade reporting, account statements, and business continuity planning.[143]

The Internal Revenue Service has concluded that digital currency should be considered "property" under the Internal Revenue Code

Other federal agencies

Numerous other federal agencies have also issued guidance or consumer advisories on digital assets, including the Consumer Financial Protection Bureau (CFPB), Board of Directors of the Federal Reserve System, and the Federal Deposit Insurance Corporation. Notably however, while the CFPB has issued a consumer advisory regarding digital currency,[144] the agency explicitly declined to include regulation of digital currency as part of its recent Prepaid Rule.[145]

Enforcement

Over the past several years, various federal agencies have stepped up their enforcement of digital asset-

related activities. Although no federal agencies have yet issued digital asset-specific regulatory regimes, such as New York's BitLicense, the agencies have prosecuted numerous individuals applying existing laws to digital asset-based activities. In some cases, these enforcement actions have been precedent-creating, such as the settlement agreement between Coinflip and the CFTC, in which the CFTC confirmed its interpretation that virtual currencies constituted "commodities" under the CEA.

Some examples of key enforcement actions include the following:

CFTC

On September 17, 2015, the CFTC settled an enforcement action against Coinflip, Inc. and its chief executive officer. Coinflip operated an online facility called Derivabit that matched buyers and sellers of bitcoin option contracts. The CFTC found that Coinflip was operating a facility for trading commodity options in violation of the CEA and CFTC regulations, including by operating the facility without having registered with the CFTC. Although the order did not carry any monetary penalties, this enforcement action was especially significant because, through the order, the CFTC established that it considered virtual currencies to be "commodities" under the CEA, and thus could exercise jurisdiction over various digital currency-related derivatives.[146]

On June 2, 2016, the CFTC settled an enforcement action against Hong Kong-based bitcoin exchange BFXNA Inc., doing business as Bitfinex. Bitfinex operates an online platform for trading cryptocurrencies. According to the CFTC, Bitfinex allowed users to borrow funds from other users to trade bitcoin on a leveraged basis, and Bitfinex did not deliver the bitcoin to the traders who purchased them, instead holding the bitcoin in wallets that it owned and controlled. Under the CEA, financed commodity transactions are required to be conducted on an exchange unless the entity offering the transactions can demonstrate that actual delivery of the commodity occurred within 28 days. Because the CFTC has deemed bitcoin and virtual currencies to be "commodities," this requirement applies to digital currency exchanges such as Bitfinex. Because Bitfinex allowed financed bitcoin transactions to be conducted off-exchange and did not actually deliver the bitcoin, it violated Section 4(a) of the CEA. The CFTC also found that Bitfinex failed to register as a futures commission merchant in violation of the CEA. Bitfinex was required to pay a $75,000 civil monetary penalty, and cease and desist from future violations of the CEA.[147]

In an enforcement action against Gelfman Blueprint and associated persons, the CFTC is using bitcoin as the jurisdictional nexus to assert its authority over the matter in light of the absence of any derivatives trading.[148] The CFTC claimed that the defendants in Gelfman fraudulently solicited investor money for a pooled fund that used a robo-trader to buy and sell bitcoin. The case is currently pending in federal court.

FinCEN

On May 15, 2015, FinCEN issued a $700,000 civil monetary penalty against Ripple Labs, Inc. for willful violations of the Bank Secrecy Act regulations. Specifically, FinCEN accused Ripple of acting as a money services business by selling virtual currency. However, Ripple did not register with FinCEN, failed to implement appropriate AML programs, and failed to report suspicious activities, among other violations.[149]

On July 27, 2017, FinCEN fined BTC-e, a virtual currency exchange, $110 million for faciliating transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking.[150]

SEC

In September 2014, the United States District Court for the Eastern District of Texas entered a final judgment against Bitcoin Savings & Trust and Trenton Shavers following an SEC enforcement action. The SEC alleged, and the court found, that Bitcoin Savings & Trust and Shavers conducted a Ponzi scheme soliciting investments in bitcoin-related investment

opportunities.[151]

In December 2014, the SEC sanctioned Ethan Burnside for operating two digital currency exchanges without registering them as either broker-dealers or stock exchanges.[152]

In June 2014, Erik Vorhees was sanctioned by the SEC for violating sections 5(a) and 5(c) of the Securities Act of 1933 for publicly offering unregistered securities in two Bitcoin-related ventures, SatoshiDICE and FeedzeBirds.[153]

In December 2015, the SEC charged two Bitcoin mining companies and their founder with conducting a Ponzi scheme. The SEC alleged that Homero Joshua Garza offered shares in a Bitcoin mining operation, but the two companies did not own enough computing power for the mining it promised to conduct. This led to "returns" for earlier investors being funded by proceeds from sales generated from newer investors.[154]

In July 2016, the SEC settled charges against Bitcoin Investment Trust and SecondMarket, Inc., alleging that the two entities violated Regulation M.[155] The settlement involved the institution of a cease-and-desist order and disgorgement of approximately $50,000 in profit.

On September 29, 2017, in a first-of-its-kind action, the SEC charged a businessman and two companies with defrauding investors in a pair of ICOs.[156] The SEC alleges that Maksim Zaslavskiy and his companies sold unregulated securities in the form of cryptocurrencies, purportedly backed by assets that did not exist. According to the SEC's complaint, investors in the companies were told they could expect sizeable returns from the companies' operations, when the companies had no real operations.

In December 2017, the SEC brought enforcement actions involving the PlexCoin and Munchee ICOs for offering unregistered securities.[157] The SEC's lawsuit against PlexCorps is pending in federal court. Munchee agreed to halt its offering and refunded the $15 million in funds it had collected from potential investors after receiving a cease-and-desist order from the SEC.

Please refer to the Applications in Capital Markets section below for additional information.

FBI/DOJ

Following an investigation by numerous agencies, Ross Ulbricht was sentenced to life in prison in May 2015 in connection with his role in Silk Road. Ulbricht founded Silk Road, an online black marketplace used to facilitate criminal activity; the site was later shut down by government task forces. Ulbricht was found guilty in February 2015 of conspiracy to distribute controlled substances, computer hacking, and money laundering.[158]

Blake Benthall, who operated Silk Road 2.0, a follow-on site to Silk Road, was arrested in November 2014 on similar charges.[159]

Charlie Shrem, a former vice chairman of the Bitcoin Foundation, and Robert Faiella, were arrested for unlawfully converting dollars into bitcoin for users of Silk Road. Each pleaded guilty in September 2014, and were sentenced to two years and four years in prison, respectively. Shrem and Faiella were charged with operating an unlicensed Money Transmitting Business (failure to register with FinCEN), money laundering, and willful failure to file SARs with FinCEN.[160]

Conclusion

The explosion of cryptocurrencies over the past several years has not escaped the attention of regulators in the United States. For at least the past several years, agencies have applied already existing laws and regulations to adapt to the digital currency landscape, notably FinCEN, the CFTC, and now, the SEC. In addition, New York's BitLicense regime became the first comprehensive regulatory regime aimed squarely at regulating digital currency. The sustained growth and prevalence of digital currencies will undoubtedly continue to solicit attention from regulators, and additional regulations and enforcement actions at the fderal and state level.

international regulation of digital currency is fast-evolving and varies substantially across jurisdictions.

International regulatory landscape

Internationally, the regulation of digital currency varies substantially by jurisdiction. Some countries have minimal regulations on the subject. Several countries have proceeded with digital currency regulation in ways similar to the United States—that is, they are currently studying the potential regulation of digital currencies, and are working to adapt and/or update their already-existing anti-money laundering ("AML") and money transmission laws and regulations to cover digital currencies. These countries include, among others, Canada, France, Italy, Singapore, and Japan.

Within Europe, the European Court of Justice ruled in late 2015 that bitcoin should be treated as a currency. This ruling stands in contrast to the U.S. CFTC's decision that digital currencies should be treated as commodities. It was thought that this ruling, along with a 2014 Opinion issued by the European Banking Authority urging an EU-wide digital currency regulatory regime, could have the effect of unifying European regulation on the subject, which has varied more substantially from country to country.

More recently, regulators across the globe have been turning their attention to Initial coin offerings (ICOs).[161] Following the SEC's July announcement, which noted that ICOs may be subject to federal securities law, regulators in Hong Kong, Singapore, China, Australia, Canada, Dubai and the UK have also given statements on this form of fundraising, with the People's Bank of China and the Financial Supervisory Commission of Korea denouncing ICOs as a form of illegal fundraising.

However, in the past, other countries have imposed much more stringent regulations, and in some cases have banned or criminalized the use of digital currencies. These more stringent laws may make it effectively impossible to deal in digital currency in various countries. For example, digital currency has been banned outright in Bolivia and Ecuador (although the Ecuadorian government has created its own state-backed digital currency). In Bangladesh, digital currency is not considered legal tender, and its use may lead to jail time.

As noted above, international regulation of digital currency is fast-evolving and varies substantially across jurisdictions. This chapter is just a sampling of notable

regulations in certain countries, and is not meant to serve as a thorough analysis of all digital currency regulations across the globe.

Europe

October 2015 European Court of Justice ruling

In one of the first major digital currency court cases impacting the European Union as a whole, on October 22, 2015, the European Court of Justice (ECJ) held that bitcoin should be treated as a currency and means of payment for tax purposes.[162] This holding stands in contrast to regulation in the United States, in which the U.S. Commodity Futures Trading Commission (CFTC) determined that digital currencies should not be treated as currencies, but instead as commodities (whereas the IRS treats digital currencies as property).[163]

It remains the case that the ECJ's ruling has major implications for all players in the digital currency space, especially from a tax standpoint. Under the EU's Directive concerning value added taxes ("VAT"), member states may not use their value added taxes to tax "transactions, including negotiation, concerning currency, bank notes and coins used as legal tender."[164] Because the ECJ held that digital currencies constitute currency and a means of payment for purposes of the EU's VAT Directive, the EU member states may not use their VAT to tax digital currency transactions. Therefore, bitcoin and digital currency exchanges that convert traditional currency to digital currency are exempt from VAT, and consumers making a bitcoin exchange would not face a VAT charge as a result of the transfer. A holding by the ECJ that virtual currencies should be treated more like commodities (in line with the CFTC) would have made transfers of fiat currency to digital currency potentially

taxable under various EU members' VATs, similar to the general tax treatment of other commodities.

The ECJ's ruling was also significant because it resolved a conflict among the member states' taxing authorities on how exactly to treat digital currency from a tax perspective—whether as a currency or a commodity. For example, while the UK tax authority had taken the position—like the ECJ—that digital currency should be treated as a currency, the tax authorities from Sweden and Germany argued that digital currency should be treated as a commodity, and thus subject to the VAT.[165]

It should be noted that this ruling applies primarily to the application of the VAT to the exchange of fiat currency for digital currency, or vice versa, or the exchange of digital currency for another type of digital currency. Sales of goods and services subject to VAT but paid for with digital currency would likely still be subject to VAT. And any capital gains on digital currency appreciation could still potentially be taxed by member states in conjunction with their income tax laws.

The European Commission's Blockchain4EU project

In February 2017, Andres Ansip, Vice President of the European Commission, noted in an official statement that "the Commission is planning to grow its support for blockchain projects."[166]

True to Ansip's statement, in June 2017, the European Commission announced the commencement of an exciting project (with a catchy title to match) – "Blockchain 4EU: Blockchain for industrial transformation".[167] The main goal of this project is to discover how distributed ledger technologies can be applied to small and medium enterprises (SMEs) in Europe.

The project will run until February 2018. Such a project personifies the European Union's approach to DLT in general. Rather than potentially stunting development by immediately ruling on the limitations and dangers of technology, the European Commission's project aims to facilitate development, which will help to inform any resultant regulatory framework.

The Commission has also set up an internal FinTech Task Force, and in April 2017 announced its plans for a "Blockchain Observatory." The aim of this project (as mandated by the European Parliament) is to build up the European Commission's technical expertise and regulatory capacity. The estimated budget for the project is half a million euros over two years.[168]

ESMA

In its February 2017 report on the application of DLT to securities markets, ESMA noted that it wanted to understand both the benefits and the risks that DLT may introduce to securities markets, and how it maps to existing EU regulation. In tandem with the European Commission's sentiment, it, too, has noted that its aim is to first assess whether there is a need for regulatory action to facilitate the emergence of the benefits, or to mitigate risks that may arise.[169]

ESMA has also importantly warned that the presence of blockchain technology "does not liberate users from complying with the existing regulatory framework, which provides important safeguards for the well-functioning of financial markets." This may come as a blow to certain market participants who believe that blockchain may provide a substitute solution to burdensome reporting obligations.

European Banking Authority and the European Central Bank

In July 2014, the European Banking Authority (EBA) issued an opinion regarding digital currency, providing recommendations to the EU Council, European Commission, and European Parliament regarding an EU-wide regulatory regime of virtual currencies.[170] The opinion also provides recommendations to national banking authorities regarding intermediate regulatory steps that can be taken to address the risks of digital currency before a full European regulatory regime is implemented.

Overall, the EBA's Opinion concluded that, although virtual currencies have the potential to create certain

benefits—particularly in the areas of reduced transaction costs and increased transaction speeds—these benefits would have less impact in the EU, because of EU directives aimed squarely at those same goals.[171] The Opinion also found that the numerous risks of digital currency (more than 70 were identified in the Opinion) would likely outweigh the potential benefits.[172]

In order to address the numerous risks of digital currency, the EBA's Opinion advocated that "a substantial body of regulation" be implemented.[173]

The European Central Bank has also produced numerous reports on DLT, including one detailing the "DLT: challenges and opportunities for financial market infrastructures," and another discussing the role of DLT in post-trading.[174] In this report, the ECB adopted a cautious stance, stating that the "technology does not yet meet the ECB's standards for safety and efficiency."

The ECB, in tandem with the Bank of Japan, stated that blockchain is not mature enough to power the world's biggest payment systems. The central banks argued that the technology has significant potential, "giving reasons to be optimistic," but said issues including latency remained, and that further development and testing were needed—showing that the technology still has some way to go.[175]

Digital currency and anti-money laundering legislation

On July 5, 2016, the European Commission adopted a proposal for a directive that, when passed, will begin to narrow the regulatory gap between the United States and the EU for digital currency exchange platforms and custodian wallet providers. Under the Commission's proposed amendments to the Fourth Anti-Money Laundering Directive (4MLD),[176] digital currency exchange platforms and custodian wallet providers will fall under the scope of 4MLD, and will be required to perform customer due diligence for all relationships. Under Article 2(3) of 4MLD, digital currency exchanges "engaged primarily and professionally in exchange services between digital currencies and fiat currencies," and "wallet providers offering custodial services of credentials necessary to access digital currencies," will be captured as entities to whom the obligations of 4MLD apply.

Many believe that this step signals the beginning of increased regulation of FinTech firms and digital currency activities in the EU, narrowing the regulatory gap with the United States.

Italy

Exactly one year after the European Commission adopted the above-mentioned proposal, the Italian AML Decree, which implements MLD4, came into force.[177] Among other things, the decree brings 'digital currencies' and 'digital currency services' within the scope of Italian AML laws. It is anticipated that the European Parliament will vote on the proposals to bring digital currencies within the scope of MLD4 in 2018. If passed, all member states will be required to bring digital currency within the scope of their respective national regimes.

Jersey

On September 26, 2016, the Proceeds of Crime (Miscellaneous Amendments) (Jersey) Regulations 2016 came into effect.[178] The regulations make virtual currency exchanges a supervised business, meaning that such an exchange must register with (and consequently comply with the rules of) the Jersey Financial Services Commission.

The Regulations define virtual currency as "any currency which (whilst not itself being issued by, or legal tender in, any jurisdiction) digitally represents value, is a unit of account, functions as a medium of exchange and is capable of being digitally exchanged for money in any form." Consistent with the European Commission's approach, the Jersey Financial Services Commission aims to treat virtual currency as a currency, as opposed to a commodity, regulating these new currencies within an existing statutory regime.

Regulatory status of cryptocurrencies in individual European countries

Generally speaking, the mining, exchanging, and buying and/or selling of goods or services with digital currency

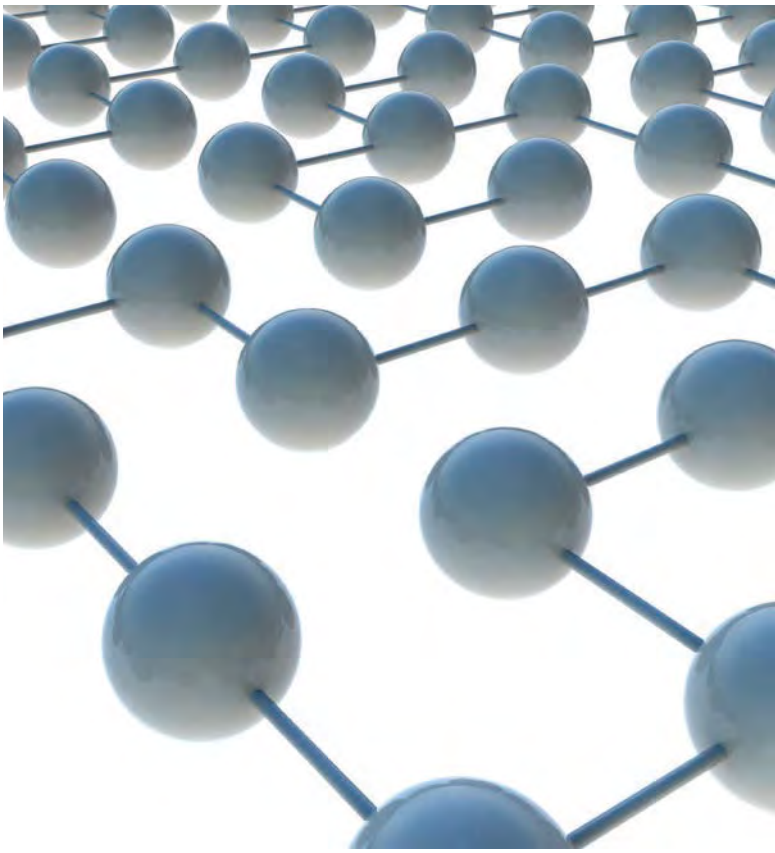
is generally legal and permitted across Europe. However, much like the United States, many European countries are currently seeking to apply existing laws to digital currency, digital currency transactions, and players in the digital currency space. For example, over the past few years, Germany, France, Italy, and the Czech Republic, among others, have explored adapting existing laws concerning money transmission, AML, taxation, and registration/licensure of financial institutions to apply to digital currency.[179]

Notable European nations that many view as having less stringent digital currency regulation include the United Kingdom and Switzerland. Many believe the United Kingdom has a relatively more favorable view of blockchain and digital ledger technology. Numerous technology incubators focusing on blockchain technology and cryptocurrencies, such as those backed by Barclays and others, are headquartered in the United Kingdom. See further detail on the FCA's regulatory sandbox below.

Further, in September 2014, the Bank of England released papers praising the potential benefits of blockchain technology and its potentially wide impact on the financial system as a whole. The Bank of England's papers note that distributed ledger technology is "the key innovation of digital currencies," and is "a genuine technological innovation which demonstrates that digital records can be held securely without any central authority." The Bank of England has also concluded that virtual currencies as a whole "do not currently pose a material risk to monetary or financial stability in the United Kingdom."[180]

In addition, many European regulators have piloted new regulatory initiatives to encourage innovation in this area. This includes the French AMF and BaFin of Germany, both of which have set up internal task forces to offer FinTech companies general regulatory guidance and assistance.

More recently, some countries have begun to transition from a proof of concept face to real-life deployment; for example, the use of blockchain on the Lantmäteriet, the Swedish land registry.[181]



On the other end of the spectrum, Russia and Iceland have each passed laws that are particularly hostile to digital currency. Legislation has been introduced in Russia that would prohibit the distribution, creation and use of "money substitutes," which includes virtual currencies; violators of the law would face criminal penalties.[182] The Russian authorities appear to be undecided with regard to the categorization of Bitcoin. Elvira Nabiullina, governor of the Russian central bank, has said it should be regulated as a digital asset, as opposed to a currency.[183]

The Central Bank of Iceland has also declared that neither bitcoin nor Auroracoin is a recognized currency or legal tender under Icelandic law, and that the purchase of digital currency is restricted under Iceland's Foreign Exchange Act.[184] The bank's position is not very clear, as it notes that "there is no authorization to purchase foreign currency from financial institutions in Iceland or to transfer foreign currency across borders on the basis of transactions with virtual currency. For this reason

alone, transactions with virtual currency are subject to restrictions in Iceland."[185]

The FCA

On April 10, 2017, the UK Financial Conduct Authority (FCA) published discussion paper DP17/3 on distributed ledger technology (FCA Discussion Paper).[186] This followed a speech by the Executive Director of Strategy and Competition at the FCA, Christopher Woolard, at the Innovate Finance Global Summit.[187] In this speech, Woolard noted that the FCA will "look to encourage innovation and adoption in technology through our RegTech work, working collaboratively to unlock the complexities and costs of regulation in new and creative ways."

The FCA's initiative on DLT follows on from its Project Innovate, which has included the creation of the FCA's 'regulatory sandbox,' whereby firms, including those developing DLT platforms, have been able to test innovative products and solutions in regulated financial services.[188] Sandbox firms include ZipZip, a cross-border money remittance platform that chooses the most efficient means for a payment to reach its destination, including via digital currencies.

The FCA Discussion Paper closed July 17, 2017. As outlined in our client alert on this paper,180 the FCA is now reviewing comments on the discussion paper with a view to publishing a summary of responses or a formal consultation paper. The consultation paper may also touch upon the subject of ICOs, which, in September 2017, the FCA denounced as "very high-risk speculative investments."[190]

Switzerland

The Swiss Federal Council published a report on digital currencies, which explains that certain businesses in the digital asset space may be subject to various Swiss laws. The Federal Council has stated that "[g]iven that virtual currencies are a marginal phenomenon and are not in a legal vacuum, the Federal Council sees no need for legislative measures to be taken at the moment. It is continuing to monitor developments in the area of virtual currencies in order for any need for action to be identified at an early stage."182

The Financial Market Supervisory Authority (FINMA) is investigating a number of ICOs for compliance with relevant laws and regulations. FINMA maintains that its regulations might apply to a given ICO, depending on the structure of the offering.

Nevertheless, Zug, dubbed "Crypto Valley," has become a hub for ICOs and is poised to continue to attract them in the future. The Federal Council report offers clear guidance to businesses that wish to set up shop in Zug, which many FinTech companies welcome, because of numerous governments across the globe wavering on these issues and providing little regulatory clarity.

Asia

Generally speaking, Asian countries have more stringent regulations governing digital currency, compared with the rest of the world. For example, the use of Bitcoin and other digital currencies is completely barred in Bangladesh, and officials from the Bangladesh Bank have stated that anyone caught using digital currencies may be sentenced to up to 12 years in jail under the country's strict AML laws.[192]

In China, while the use of bitcoin and digital currencies by individuals technically remains legal, its use is difficult, if not impossible. This is because in December 2013, the People's Bank of China (PBoC)—together with the Ministry of Industry and Information (MIIT), China Banking Regulatory Commission (CBRC), China Securities Regulatory Commission (CSRC), and China Insurance Regulatory Commission (CIRC)—jointly issued a notice (the "2013 Notice") on risks of bitcoin and warned financial institutions, payment institutions, and third-party payment providers, that they may not accept, use, or sell digital currencies; may not generally be involved in digital currency transactions; and may not work with digital currency-related businesses.[193]

The 2013 Notice viewed bitcoin as a special type of "virtual goods." While financial institutions and third-

party payment providers are prohibited from dealing in bitcoin, bitcoin online trading platforms are not banned from providing services for bitcoin trading. Bitcoin online trading platforms are required to comply with anti-money laundering obligations by implementing user real-name registration and suspicious transaction reporting measures.

In wake of the eye-popping growth of ICOs (see details below) in China in 2017, the PRC regulatory authorities have become increasingly more concerned about the risks of illegal fund-raising activities involved in ICOs. On September 4, 2017, the PBoC, Office of the Central Leading Group for Cyberspace Affairs, the MIIT, the State Administration of Industry and Commerce (SAIC), the CBRC, the CSRC, and the CIRC jointly issued a notice (the 2017 Notice) on prevention of financing risks by offering tokens.

The 2017 Notice states that ICOs in their nature are illegal public fund-raising and involve illegal offering of token, illegal offering of securities, and illegal fund-raising, financial frauds, Ponzi schemes and similar criminal offenses. The Notice reiterates the position under the 2013 Notice that tokens or "virtual currencies" that are offered or raised in ICOs shall not be recognized as legal tender or to be used as such in the market.

As from September 4, 2017, the 2017 Notice requires all ICO activities to immediately stop. Platforms for token financing and trading are prohibited from (1) exchanging legal tender to token, "virtual currency" or vice versa, (2) buying or selling of or acting as central counterparty for token or "virtual currency," or (3) providing pricing or information services for token or "virtual currency." Websites and mobile apps of unlawful token financing and trading platforms shall be closed down or removed from app stores.

While the 2017 Notice primarily aims at ICOs and ICO platforms (such as ICOAGE, ICO365, ICOINFO), the above rather sweeping prohibition could potentially be interpreted to ban trading platforms for Bitcoin or other "virtual currencies." It remains to be seen how PRC authorities would implement the 2017 Notice in practice.

The regulatory status of digital currency in Thailand is far from clear: in 2013, the Bank of Thailand informed a digital currency-based business that digital currency activities were illegal in Thailand; however, one year later, the same bank reportedly concluded that Thai law does not regulate digital currency, but that exchanges still could not operate if they could not prevent digital currencies from being exchanged with currencies other than the Thai Baht.[194]

On the other end of the spectrum, Japan stated in June 2014 that, despite the fall of Japanese-based bitcoin exchange Mt. Gox, the country would not move to regulate virtual currencies in the immediate future.[195] Japan then appeared to struggle with how to handle digital currencies for a few years, but, in 2017, seemed to make the decision to embrace the market. The Japanese government recognized bitcoin as legal tender in April 2017 and, in September 2017, Japan's Financial Services Agency officially recognized 11 companies as registered digital currency exchange operators.

12

under the country's strict AML laws, the number of years that officials from the Bangladesh Bank have stated that anyone caught using digital currencies may be sentenced to.

On the other hand, the Financial Services Commission, South Korea's financial regulator, recently banned the raising of funds through ICOs.[196]

Several other Asian countries, such as India and Singapore, are pursuing a more cautious approach similar to Europe and the United States, where they are seeking to adapt already existing laws to cover virtual currencies.[197] Considering the vastly different treatment digital currencies receive jurisdiction to jurisdiction, digital currency issuers must consider the laws of each jurisdiction where buyers may reside to properly manage regulatory risk.

The Americas

Outside of the United States, two countries in the Americas hold "first" status in digital currency regulation: Canada became the first country in the world to enact a national law specifically regulating virtual currencies, while Ecuador became the first country to issue its own state-backed digital currency.

In June 2014, Canada amended its Proceeds of Crime (Money Laundering) and Terrorist Financing Act to include provisions specifically governing virtual currencies from an AML perspective.[198] Pursuant to the amended statute, dealers in virtual currencies would be subjected to the same regulations as money services businesses.[199] The implications of this classification are that those dealing in virtual currencies would be required to register with the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC," similar to FinCEN in the United States), and abide by various regulatory obligations surrounding recordkeeping, suspicious transaction reporting, and verification procedures, among others.[200] Under the revised statutes, banks are also prohibited from opening or maintaining banking relationships with unregistered businesses that are now classified as money services businesses on account of dealing in digital currency.[201]

Second, in 2015, Ecuador became the first nation to issue its own, state-sponsored digital currency—the dinero electrónico—that is officially legal tender in the country alongside the U.S. dollar.[202] However, although the Ecuadorian government's own digital currency is legal tender, Ecuador has explicitly banned Bitcoin, Ripple, and other types of digital currency.[203] Bolivia has a similar ban on digital currency, but has not issued its own digital currency as a substitute.[204] Perhaps because of these bans issued by their South American neighbors, authorities in Argentina and Brazil have issued warnings about the risks of using virtual currencies not recognized as legal; however, these countries have not banned digital currency themselves.[205]

Middle East

The Middle East, particularly the United Arab Emirates ("UAE"), has taken major steps over the past five years to catapult itself into the digital age—especially with global trends in financial technology. Within the Middle East, the UAE plays a lead role in fostering innovation and encouraging the development of new processes and methods to build smarter cities throughout the region. Recent press announcements, for example, reflect that it is among the first in the region, and possibly in the world, to set the stage for blockchain adoption at a governmental level, and to move toward establishing a legislative framework to accommodate this adoption. Despite announcements to this effect, however, the UAE's position on digital currency in general, and on Bitcoin in particular, is currently an area that remains unclear.

Under the UAE's Regulatory Framework for Stored Values and Electronic Payment Systems, "all virtual currencies (and any transactions thereof) are prohibited." However, the UAE Central Bank clarified that the regulation does not cover cryptocurrencies. In a public statement, the governor of the UAE Central Bank explained that these regulations do not cover "any type of digital unit used as a medium of exchange, a unit of account, or a form of stored value. In this context, these regulations do not apply to bitcoin or other digital currencies, currency exchanges, or underlying technology such as blockchain."[206]

The government is yet to release official guidance on whether it views bitcoin as a currency or a commodity, which could potentially determine how it would also be treated for value added tax purposes. If the determination is that bitcoin is to be treated as a commodity, then its regulation will fall within the ambit of the UAE Securities and Commodity Authority; whereas if it is treated as a currency, its regulation would fall under the UAE Central Bank's regime.

Though the government is yet to issue definitive guidance on the matter, a degree of comfort and certainty has been provided by the UAE Central Bank. The governor of the UAE Central Bank, His Excellency Mubarak Rashed Khamis Al Mansouri, has stated that current regulations do not apply to "bitcoin or other crypto-currencies, currency exchanges, or underlying technology such as Blockchain."[207] The UAE Central Bank has also taken active steps to explore how blockchain might facilitate a transformation in conventional trading, the settling of accounts, investment and asset management.

Dubai, an Emirate within the UAE and one of the leading financial centers of the Middle East, has unveiled the "Dubai Blockchain Strategy" as a part of a joint effort to transition Dubai into becoming a "smart city" by injecting blockchain technology to the city's public and private sector infrastructures. Initiated by "Smart Dubai," a governmental agency tasked with enhancing Dubai's quality of life through technological innovation, the effort aims to use blockchain technology to boost government efficiency for both citizens and non-citizens by filing, processing, and transacting governmental documents, such as visas and licenses, through the use of distributed ledger technology. The Dubai Blockchain Strategy also hopes to boost industrial growth by introducing a blockchain-based system that would encourage and enable the creation of new businesses in various industries using blockchain technology. For

Smart Dubai envisions Dubai to be completely running on blockchain technology by the year 2020

example, Smart Dubai already launched a city-wide pilot in March 2017, and envisions Dubai to be completely running on blockchain technology by the year 2020.[208]

The UAE Global Blockchain Council was launched in February 2016 and has received support from key stakeholders within the UAE government, financial services, and telecommunications sectors. The council aims to help the authorities better understand blockchain technology and its regulatory implications, along with the undertaking of pilot projects to test the readiness of markets to adopt digital currencies. The Dubai Supreme Legislation Committee stated that "the present and future of the legislative and legal frameworks related to crypto-currency known as Bitcoin" is a signal that the UAE is seeking to develop a mature regulatory environment for the use of bitcoin, crypto-currency and Blockchain technology.[209]

Other countries in the Middle East, such as the Kingdom of Saudi Arabia, Kuwait and Israel, have also introduced the world of bitcoin to its citizens. The report "Disruptive Technology: Bitcoins, Currency Reinvented?" recently issued by a Kuwait-based investment banking and asset management firm known as Markaz, has taken a step further stating that oil producing countries, particularly in the GCC, could benefit if bitcoin is used in trading.[210] Currently, Bitcoins are available in Kuwait online by connecting to Bitfils.com.[211]

In the Kingdom of Saudi Arabia, digitization is expected to play a central role in that nation's recently announced National Transformation Plan, aimed at overhauling its entire economy over the next 10 years to wean the nation off its almost absolute reliance on oil & gas production as the foundation of its economy.[212] This is in line with Saudi Arabia's vision of developing a vibrant digital economy by 2030. For this purpose, the Saudi Arabian Monetary Authority is taking steps to provide the legislative framework for the use of bitcoin. Moreover, the Saudi Arabian central bank is working with the UAE central bank to test a new digital currency for cross-border payments.[213]

The Kingdom of Bahrain has been targeting "country level" blockchain adoption and has been working along with the central bank of Singapore in a plan to build a pilot blockchain project within its borders.[214] The Monetary Authority of Singapore (MAS), along with Singapore's stock exchange and eight local and foreign banks, have been developing a project to use blockchain technology for interbank payments. Following this, Bahrain is looking to develop its own blockchain trial, as the government works toward establishing a robust and comprehensive regulatory regime in the digital currency space. That is to say, the development of a "regulator-friendly space" that will allow research and testing of new FinTech products and innovations that it believes the Middle East region requires.

Oman and Qatar have also made progress in their blockchain usage and development. On April 30, 2017, The National Bank of Oman and Commercial Bank of Qatar confirmed the completion of a blockchain pilot for the use of international remittances.[215] This was part of a larger initiative launched by the Commercial Bank of Qatar in 2016 with other parties, including the United Arab Bank and banks in India and Egypt. Prior to this, the Commercial Bank of Qatar conducted a separate trial with banks across the Middle East, which saw participants sending each other payments as part of a bid to develop new remittance channels in established payment corridors in the Middle East.

Israel, driven by a strong defense industry, military, and cutting-edge academic institutions, has become a hub for startups and hi-tech innovation. The country's unique experience with FinTech, cybersecurity and cryptography has positioned Israel as a fount of blockchain innovation.

Israel's government is set to apply capital gains tax to bitcoin sales, categorizing digital currencies as a type of property. On January 2017, the Israel Tax Authority (ITA) said that it would consider bitcoin and other digital currencies as a kind of intangible asset, rather than as a foreign currency.[216] Profits would then be taxed at the capital gains rate, which in Israel begins at 25 percent. Further, any commercial sales of bitcoin or transactions involved with trading are subject to value added tax.

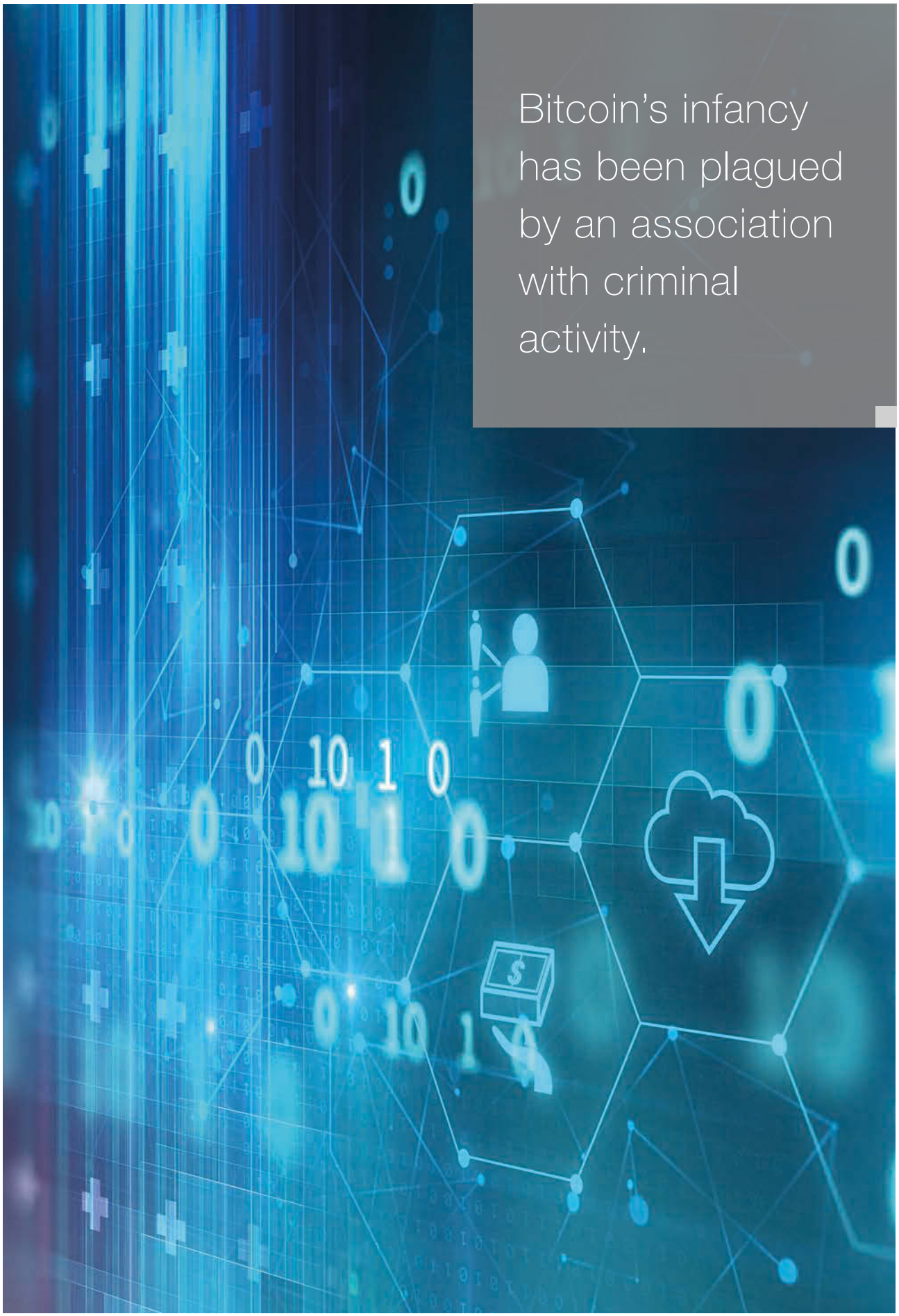
In Israel, "Bits of Gold" has been providing bitcoin exchange services since 2013.[217] Users can buy bitcoin using bank transfers, credit cards or cash. Customers can open an order on the "Bits of Gold" website and can deposit money at any one of its locations. Alternatively, they can use the Bitcoin ATM located at the Bitcoin Embassy in Tel Aviv. However, in 2017, the Tel Aviv district court released a regulation stating that banks can legally deny service to bitcoin business in Israel on the basis that hackers could break into its accounts in order to fraudulently send funds from the bank to buy bitcoins.[218]

Africa

There is limited data on the regulation of digital currency throughout Africa.[219] In South Africa, a joint statement issued by the National Treasury, the South African Reserve Bank, the Financial Services Board, the South African Revenue Service, and the Financial Intelligence Centre, confirmed that "[c]urrently in South Africa there are no specific laws or regulations that address the use of virtual currencies."[220] Therefore, the use of the digital currency in the country is generally permissible. However, the same authorities warned against the risks of digital currency, and also clarified that because of this unregulated status, "no legal protection or recourse is afforded to users of virtual currencies," and "virtual currencies cannot be classified as legal tender as any merchant may refuse them as a payment instrument."[221]

In July 2017, however, the South African Reserve Bank (SARB) announced that it will begin to test a number of regulations related to digital currency toward the end of 2017.[222] Tim Masela, head of the National Payments Systems at the SARB, has said that the country would be open to issuing a national digital currency.[223] This would follow in the footsteps of Tunisia, which in 2016, put its national currency on a blockchain.[224]

As there are significant areas in Africa lacking extensive infrastructure, entrenched financial institutions, a high degree of political stability and/or large pools of capital, there are many opportunities for the growth of blockchain technology solutions for these regions. Numerous payment remittance companies are experimenting with blockchain technologies in order to provide cheaper and more efficient money transfers to underbanked and unbanked areas, for example. African nations so far are not inhibiting these innovations, and blockchain adoption is growing within Africa.



Bitcoin's infancy has been plagued by an association with criminal activity.

Insuring digital currency and digital currency business

Companies that service the digital currency industry and its holders face risks unique to the digital currency[225] market, as well as to the financial services market generally. Thus, key questions for potential policyholders include how, if at all, insuring bitcoin or other digital currencies is different from insuring other currencies? What insurance products currently exist that may cover bitcoin holders, servicers, and third-party vendors, and is the industry developing new types of coverage specific to digital currency? And, to date, how has the insurance industry responded to claims made under those insurance policies? In addition, companies that do not service the digital currency industry may be called upon to utilize digital currency in connection with insurance claims. This chapter examines these questions and identifies practical concerns and tips for policyholders.

Insurance and underwriting issues

Bitcoin is both an asset akin to currency and a protocol for digitally recording transactions. Viewed from this (simplified) perspective, insuring bitcoin holders, storage providers, exchanges, or related companies should be no different in terms of risk than any other business that safeguards or transfers an anonymous or fungible commodity, like cash, or that must protect its trade secrets or sensitive digital information. A variety of "traditional" insurance coverages exist, for example, to insure financial institutions and technology companies and their management, including network security and privacy liability (cyberliability) insurance, financial institution bonds and commercial crime insurance, directors' and officers' liability (D&O) insurance, and professional liability (E&O) insurance. At least one court has characterized bitcoin as equivalent to traditional assets like "money" or "securities."[226] Similarly, the IRS has concluded that digital currency should be considered "property" under the Internal Revenue Code,[227] and the CFTC treats bitcoin and other virtual currencies as "commodities" for regulatory purposes.[228]

These determinations suggest that traditional insurance ought to respond to risks faced by the digital currency industry, just as insurance responds to similar risks in more established financial and technology industry sectors.

But novel issues abound, because digital currency (and, for example, derivatives) features several unique characteristics. Unlike most "traditional" currencies, bitcoin requires no financial institutions to issue new currency and no banks to store it, and transactions may be anonymous and are non-reversible. Also, because bitcoin is decentralized, and its software is open-source, there is limited control over the currency or technology beyond a core group of developers and dedicated individuals. Thus, bitcoin raises potentially unique issues with regulation, information security, price volatility, and reputation.

Regulation

As discussed in the U.S. and International Regulatory Landscape chapters above, governments have taken divergent approaches to regulating digital currencies, with some outright banning cryptocurrencies altogether.[229] The possibility remains that governments will impose substantial regulatory burdens or penalties on companies operating within the industry, including the risk of fines, application of anti-money laundering laws, and rigorous oversight by government agencies that range in focus from consumer protection to commodities regulation. Traditional insurance policies should be reviewed carefully to determine whether they may cover regulatory investigations or actions, and whether any such regulation implicates generally applicable exclusions,

Information security

The digital currency industry is seeking consensus on how best to secure bitcoin and other cryptocurrencies, and the companies that service digital currency holders, including storage companies, trading platforms, and exchanges. Ownership of digital currency is synonymous with knowing a private "key" associated with an address on the public chain of title (the "blockchain"). To conduct transactions, owners may use the services of a company acting as an intermediary to secure its private keys and run the software needed to spend bitcoin. These companies take varied approaches to securing private keys in their possession. Some put private keys in "cold storage," meaning keys are saved in computers not connected to the public Internet. Other companies utilize (among other methods) "multi-sig" technology that requires knowledge of multiple keys before a transfer of bitcoin is possible, with the company holding one key, the owner another, and a third retained offline as a backup. Thus, neither the industry serving bitcoin users nor the users of the currency have yet identified preferred standards of asset protection.

Price volatility

Bitcoin has risen and fallen in price dramatically since its introduction. Price volatility raises issues with the financial strength of insured companies, the severity of the risks they face, and how to predict or quantify losses.

Reputation concerns

Bitcoin's infancy has been plagued by an association with criminal activity. Media reports often discuss bitcoin in connection with cybercrime, including schemes to defraud, phishing attacks, and theft. A recent explosion of cyber extortionists threatening cyberattacks, the disclosure of confidential information, or the interruption of networks in order to demand payment in the form of virtual currencies, has also drawn attention to Bitcoin and other cryptocurrencies. Bitcoin has likewise reportedly been used by criminals as an anonymous means of payment for drugs and other illegal activities.

Given these issues and concerns, what can companies operating within the bitcoin economy expect? In short, a rigorous insurance underwriting process, and potentially a rigorous claims process when losses ultimately occur. Insurers may assess a company's current practices and protocols concerning data, network and privacy security, physical protections

for data held in cold storage, and breach or loss response. In the event of a loss, insurance policies may require rapid identification and quantification of the breach or loss, collection and preservation of information, mitigation of any damages or losses, prompt notification to the insurance carrier, and potentially even consent from the insurance carrier to take any further action, such as payment of a cyber extortion ransom. Because of the sensitivity of the information a policyholder may be required to share with insurers, both during the underwriting process and in the event of a loss, companies should insist on signing strong confidentiality agreements with insurers and brokers. Coverage counsel can help policyholders navigate these and other related issues both during placement of coverage and after a loss occurs.

Potential insurance coverage under traditional policies

Although bitcoin raises a number of novel issues, insurance companies may seek (and have sought) to insure the risks arising from this technology with well-established forms of coverage. Some insurers also have begun developing hybrid forms of insurance coverage to address both the more traditional risks associated with the industry, and the unique aspects of bitcoin and bitcoin technology.

Cyberattacks and ransomware

Cyberliability insurance is designed to address first-party losses and third-party liability as a result of data security breaches, and the disclosure of or failure to protect private information. It commonly insures against (or helps defray) the cost of misappropriated data, investigating a breach, responding to regulators, defending against lawsuits, notifying affected persons, restoring or recreating any lost data, responding to cyber extortion demands, and paying damages and settlements, among other expenses. Cyberliability policies often are negotiable and may be tailored to a particular company or industry.

Ideally, a cyberliability policy intended to cover bitcoin or bitcoin-related operations should be drafted broadly enough to cover issues unique to the currency and technology. The policy thus might insure against liability related to the company's storage or exchange of bitcoin, corruption or breach of its associated technology, or losses as a result of a compromised vendor. The definition of a security breach or privacy event should be broad enough to include disclosure of or damage to the types of confidential information unique to bitcoin, including users' private keys. Security concerns or vulnerabilities particular to bitcoin and bitcoin technology also should be addressed where possible, including the generation of flawed keys, transaction malleability attacks, 51 percent attacks intended to manipulate the blockchain, sybil attacks, and distributed denial of service attacks.[230]

Following a wave of recent "ransomware" cyberattacks—which routinely demand payment in bitcoin or other digital currency in exchange for terminating the attack—businesses should also confirm that their cyberliability policies include cyber extortion or ransomware coverage. While cyber extortion coverage is widely available in the market and included in many policies, companies should review the terms of these provisions carefully. For example, the policy should cover payments to obtain bitcoin or other digital currency to be paid as ransom. Whether an insured is required to obtain consent from its insurer before a ransom demand is paid should also be taken into account. In addition, companies should also study whether (and how much) coverage is provided for forensic expense costs and any business interruption caused by the extortion. A number of cybersecurity consulting firms have also started to offer "ransomware" services, where they will analyze the malware and assist customers with the bitcoin negotiations and/or payments.

Financial institution bonds and commercial crime policies

Bonds and commercial crime policies generally insure against first-party losses of money, property and securities caused by certain types of criminal, fraudulent or dishonest activity, including employee dishonesty, fraud, forgery, and certain types of extortion. Many bonds and commercial crime policies contain coverage for computer crimes and frauds that directly result from the use of a computer, and result in the transfer of money, property, or securities from within the company to parties outside of the company.

Businesses that use, keep, or perform services related to bitcoin should ensure that bitcoin and/or digital currency is included in the definition of "money," "currency," "property" or any related terms or definitions that identify covered types of loss.[231] Bitcoin transactions may be conducted "peer-to-peer," meaning the buyer and seller do not need to use a central exchange. Companies should examine their potential exposure to losses arising from peer-to-peer transactions, because at least one insurer has publicly stated that peer-to-peer transactions are not covered under its commercial crime policy form.[232] Businesses seeking to insure against digital currency-related losses under commercial crime policies should also be aware of revisions in the Insurance Services Office's (ISO) Commercial Crime Program that became available in November 2015. Those revisions add a "virtual currency exclusion" to the ISO form, which excludes losses involving virtual currency of any kind.[233] Coverage for virtual currency can be added back in through the ISO's optional endorsement titled "Include Virtual Currency as Money," which reintroduces coverage for virtual currency under the form commercial crime policy's Employee Theft and Computer and Funds Transfer Fraud insuring agreements.[234]

Social engineering and "phishing"/"fraudulent impersonation" attacks also are a threat to a bitcoin business. A bad actor could seek to convince an employee that they are conducting a genuine transaction or sharing private information with a trustworthy recipient, when the employee is in fact an unwitting intermediary in a scheme to defraud. Social engineering attacks can implicate the "direct" causation and intent standards in many bonds and commercial crime policies. Traditional financial institution bonds cover only losses "directly caused" by a covered activity. The "direct loss" standard is not uniformly interpreted by the courts, and is a frequent source of insurance disputes. Some courts hold that the "direct loss" standard is equivalent to proximate causation under traditional tort law, but others hold that "direct loss" means that there can be no intervening cause between an action intended to cause harm and the harm itself. If the latter interpretation applies, it may be difficult to obtain insurance proceeds for losses caused by a social engineering or phishing attack on a bitcoin company.

A recent lawsuit filed by bitcoin payment processor Bitpay, Inc. against its commercial crime insurer illustrates this issue.[235] After a phishing attack compromised the email account of a Bitpay executive,

the hacker used information collected from the executive's email to induce the company to transfer funds to an ostensible customer wallet that was, in fact, controlled by the hacker. Bitpay's commercial crime insurer denied coverage, asserting that because the Bitpay executive acted as an unwilling intermediary in the scheme, the loss was not "directly caused" by the activity of the hacker. In addition, even though the definition of "money" in Bitpay's crime policy had been specifically amended to include bitcoin, Bitpay's insurer also asserted that the loss was not insured because bitcoin exists only in electronic form and cannot be transferred from inside Bitpay's premises to outside the premises.

Based on public court filings, Bitpay and its insurer appear to have reached a settlement before any substantive rulings were made on the coverage issues raised in the case. Recent decisions from other courts, however, highlight a continued split in the case law on whether social engineering attacks are covered as "direct loss" under traditional fidelity or commercial crime policies.[236] For this reason, businesses should consider adding a specific social engineering fraud endorsement to their crime policy, which is now offered by several insurers.[237]

Many commercial crime policies also require "manifest intent" by an employee before a loss caused by employee dishonesty is insured, a phrase sometimes interpreted by courts to mean that an employee must not only intend to personally gain from his or her dishonesty, but also to intend to harm the company. Thus, an insurer may assert a defense to coverage if a defalcating employee's intent was directed at the bitcoin holder, not the company.

In addition, some courts have questioned whether the use of email to fraudulently impersonate a known person or coworker constitutes the use of a computer for purposes of computer fraud insuring agreements.

D&O insurance

D&O insurance is designed to protect a company's directors and officers, and often to a more limited extent, the company, against third-party liability. D&O policies commonly insure individual directors and officers when they cannot be indemnified by their

companies ("Side A" coverage), the company when it pays indemnification to its directors and officers ("Side B" coverage), and the company in connection with lawsuits alleging violations of the securities laws ("Side C" coverage). Monetary damages may be covered, but property damage generally is not. D&O insurance often can be negotiated.

Although a variety of D&O policy provisions should be tailored to bitcoin-related risks, three are of particular note. First, any bitcoin-related company should ensure its policy will cover securities lawsuits triggered by a loss of bitcoin or damage to the company's bitcoin operations. Second, given the prevalence of criminal activity related to the currency and technology, as well as the uncertain regulatory environment, the insurance policy should clearly insure the costs of cooperating with government investigations, inquiries, and any administrative proceedings related to bitcoin. Finally, companies should pay attention to any exclusion for loss arising from professional services provided by the company.

E&O insurance

E&O insurance is designed to protect individuals and companies from liability for mistakes, omissions, and other errors made in the performance of professional services. E&O polices can be tailored to specific professions and risks, and are frequently negotiable. Every company that provides services related to bitcoin in return for a fee – whether they host or maintain customer "wallets," operate exchanges, facilitate transactions, or provide any of the myriad services relevant to the industry – can potentially benefit from having E&O insurance. A lawsuit accusing a company of an error, even if frivolous or baseless, could result in substantial legal expenses and reputational damage.

Would a traditional E&O policy cover a financial institution utilizing new bitcoin technology, such as a financial institution implementing blockchain technology, to record and maintain the ledger of private stock transactions? Although many E&O policies broadly define what constitutes covered "professional services," E&O policies are not uniform among different insurers, and different industries and may be tailored to specific risks, and thus the definition of "professional services" may or may not automatically include such services. For instance, many E&O policies issued to financial institutions define "professional services" simply as those services provided by the insureds to a customer or client for a fee or other form of compensation or services. In some cases this language may be read to capture all such services provided by the policyholder (i.e., any service performed for a customer for a fee); but for other policyholders, this generalized description of "professional services" may be tied, either explicitly or implicitly, to particular representations made in the company's application for the insurance, or in the company's public filings with the SEC or other regulators. Further, the definition of "professional services" in some E&O policies may incorporate or list specific types of services performed by the particular policyholder. Accordingly, companies performing bitcoin-

companies performing bitcoin-related services should carefully review the way in which their E&O insurer defines covered professional services

related services should carefully review the way in which their E&O insurer defines covered professional services to decrease the possibility of a coverage dispute in the event of a loss.

Kidnap and ransom (K&R) insurance

K&R coverage insures an individual or company from loss in the event the insured, an employee, or some other identified person is kidnapped, detained, or ransomed. K&R coverage is an indemnity product, meaning that the ransom money must first be paid before the insurer will provide reimbursement. According to recent media reports, bitcoin has emerged as a preferred currency for kidnappers and extortionists. As such, companies should ensure, where possible, that its K&R coverage allows for ransoms and extortion payments to be paid in bitcoin or for reimbursement of money used to purchase bitcoin. For example, any definition of "money" or "currency" in the policy should expressly include "bitcoin."

Bitcoin-specific insurance

Several major insurers reportedly have developed specialized insurance products for the bitcoin market. Although the details, terms and conditions of these policies are not widely known, it has been reported that at least one major carrier has created an E&O policy with the privacy and data protection elements of cyberliability coverage, commercial crime protection, and deposit protection;[238] and another has developed a "new" type of commercial crime coverage specific to bitcoin.[239]

Other companies have created captive insurance funds to protect their customers instead of turning to insurance companies. [240] As this nascent industry and its technology continues to develop, it remains to be seen how these initial insurance products will respond to the unique risks posed by bitcoin, and the industry that serves the currency and its users.

The bottom line

Bitcoin has created a small but growing industry focused on, among other things, securing users' private keys, facilitating transactions, running bitcoin exchanges, and trading bitcoin futures or swaps. In order to increase customer and investor confidence, and to free capital to grow their businesses, companies providing digital currency-related services may, like the financial services industry supporting "traditional" currencies, look to transfer their risk of liability and loss through the purchase of insurance. Until insurance policies and products specifically tailored to the industry are widely available to companies providing digital currency-related services, companies should review their current insurance coverage to assess how and to what degree insurance will respond in the event of common claim scenarios. Companies purchasing either traditional policies or bitcoin-specific coverage for the first time should carefully review the terms and conditions of any proposed coverage, and consult with a reputable broker and policyholder coverage counsel when comparing different policy forms and negotiating important changes and enhancements where possible.

Transactions involving the blockchain have the potential to be significantly more efficient.

Applications in capital markets

Although it was developed in the context of creating digital currency, the blockchain has the potential to have a major impact on both financial institutions and financial transactions involving fiat currency. In fact, few Bitcoin-related developments generated by financial institutions have to do with trading bitcoins or conducting transactions involving other digital currencies. Instead, these institutions are applying the technology behind bitcoin—the blockchain—to numerous types of other financial innovations that do not involve any type of digital currency.

For the past few years, banks and financial institutions have met to discuss how to respond to and/or utilize this technology, and several financial institutions are performing in-house experiments and projects seeking to take advantage of the blockchain's benefits.[241] Several tech startups, such as Digital Asset Holdings, led by Blythe Masters; and R3, which is supported by Wells Fargo, Barclays, Credit Suisse, and Bank of America, among others, are also exploring the blockchain space, and seeking to find ways to implement blockchain technology into everyday banking and financial transactions.[242]

Some analysts are hailing blockchain technology as transformative, with Accenture describing it as possibly the "critical backbone" of the future capital markets infrastructure,233 and the New York Times describing it as a "fundamentally new way" of transacting and maintaining records.[244] Financial industry consultancy firm Greenwich Associates interviewed 102 institutional financial professionals in mid-2015; of those surveyed, 94 percent responded that they believed that blockchain technology could be applied in institutional markets, and almost half reported already being in the midst of reviewing the technology within their firms.[245]

A separate survey from Greenwich Associates found that as much as $1 billion was invested in blockchain initiatives related to capital markets in 2016,236 up from an estimated $75 million in 2015, according to consultancy firm Aite Group.[247]

While there are those who are more skeptical,

industry professionals, including major financial players, have demonstrated a keen interest in applications of blockchain to their industry.

Greater efficiencies

Transactions involving the blockchain have the potential to be significantly more efficient. This increased efficiency comes in the form of quicker settlement, improved accuracy, lower error rates, automated settlement, and significantly less reliance on third parties for post-trade settlement. Such efficiency may lead to lower costs for all parties involved.

One of the most exciting potential applications of the blockchain in capital markets is the possibility of using it to eliminate the cost and time of clearing and settling financial assets. Because the blockchain is decentralized and is not maintained by any one party, two parties can exchange an asset or information directly with each other without the use of a third party validating the information, in a near instantaneous settlement. In the blockchain, the assets can be tied to individuals, with no need for institutional custodians.

This development could save Wall Street banks and investors billions of dollars by radically reducing a transaction's lifespan, as it would free up capital that is otherwise pledged to back trades until they are settled. Typical securities trades take two to three days to settle.[248] Additionally, the potential savings for other transactions is even greater. For example, the average bank loan took nearly 19 days to settle in 2016.[249]

Initially, the blockchain is most likely to impact asset transactions where there is no central clearing or trading authority, such as transactions involving FICC derivatives, syndicated loans, and private investments. In 2015, NASDAQ unveiled the use of its Nasdaq Linq blockchain ledger technology to successfully complete and record private securities transactions for Chain.com, the inaugural Nasdaq Linq client. In May 2017, Nasdaq and Citi announced an integrated payment solution based on Chain's blockchain technology, which overcomes the challenges of liquidity in private securities by streamlining payment transactions between multiple parties.[250] Additionally, other international exchanges, including the Australian Stock Exchange, Japan Exchange Group, Korea Exchange, Moscow Exchange and London Stock exchange, have launched blockchain initiatives to improve their operations.[251] Beyond exchanges, in January 2017, Depository Trust & Clearing Corporation successfully completed the testing of blockchain-based technology for the clearing and settlement or repurchase agreement transactions,[252] and in April 2017, as a member of a working group of seven firms, successfully tested blockchain and smart contracts to manage post-trade lifecycle events for standard North American single-name credit default swaps.[253]

In addition to improved efficiency, the security provided by the blockchain may have an even greater impact on markets with high transaction volume, but less trading infrastructure in place, such as loans and private over-the-counter derivatives that cannot be backed by clearinghouses.

For example, numerous companies are experimenting with using blockchain technology with trade finance platforms. In early 2017, seven European global banks, including Deutsche Bank and HSBC, joined to form the "Digital Trade Chain" (DTC) consortium, using IBM to develop their blockchain-based trade financing platform.[254] The platform aims to fill financing gaps hampering domestic and cross-border trade for small and medium-sized businesses ("SMEs") by providing more transparent, simplified, efficient, and secure, paperless trade financing services to such SMEs conducting transactions. The banks hope that by conducting trade financing on a distributed ledger, transactions recorded on the ledger would promote accountability and also allow businesses easier access to their records and finances without the need to endure the more tedious and time-consuming traditional processes involved in authorizing and clearing trade transactions.

More security and transparency

Many analysts believe that the blockchain can make financial transactions more secure. Because the blockchain is not controlled by a central party, but instead involves decentralized control, the blockchain is less vulnerable to (if not immune from) cyberattack. The blockchain cannot be lost or corrupted by participants, and thus counterparty risk in transactions is significantly reduced.

Because of the public nature of most blockchains, and the completeness of the information contained in a digital ledger, the blockchain also has the future potential to more easily facilitate data-sharing for KYC and AML purposes, trade surveillance, regulatory reporting, collateral management, and perhaps even real-time auditing of transactions.

However, despite the blockchain being publicly available and easily shared among parties, various identifying information about parties making transactions may be hidden and made private in certain circumstances. There is thus a means to limit privacy risks in conjunction with the improved transparency.

Imagine also reconfiguring on the blockchain various protocols widely used in the capital markets, such as SWIFT (a communications platform designed by the Society for Worldwide Interbank Financial Telecommunications to facilitate the transmission of information about financial transactions), or FIX (a trading platform for communicating trade information based on the Financial Information eXchange Protocol). Considering that, on average, current cross-border transactions have settlement periods of three to five days and error rates of nearly 12.7 percent,245 blockchains may minimize, if not eliminate, disputes or errors in such transactions due to the blockchain's ability to record the complete history of all transmissions.

Consortiums

While the main differences between "open" and "closed" blockchains have been previously touched upon, consortiums almost represent a hybrid of the two. Predominantly "closed" in nature, blockchain consortiums are formed when several entities, typically within the same or related industries, unite to create a unified platform on a distributed ledger in order to advance their industries through the use of distributed ledger technology.

Perhaps the most talked about blockchain consortium, the R3 consortium, expanded from its original nine members in 2015 to more than 80 members of global financial institutions in 2017. R3's aim is to develop and sync the coalition of world banks on a distributed ledger platform in order to reap the benefits technology can present to the banking industry, such as safer intra-bank efficiency and lower transaction costs. In May 2017, R3's fundraising efforts hit a record-breaking $107 million from investors, making it the largest dollar amount ever raised for distributed ledger technology.

Although much hype and momentum surrounds R3, several big banks such as Goldman Sachs, Santander, and Morgan Stanley have already left the consortium. While most of those former members

withdrew in late 2016, before the R3's fundraising efforts began to accelerate, JPMorgan Chase declared its exit from the alliance just a month before R3's record success in pursuit of other blockchain investments and consortiums. One such consortium is the Enterprise Ethereum Alliance (EEA), which JPMorgan, along with other banking and tech giants, formed in February 2017 in order to implement the use of a business-friendly version of Ethereum, which according to its website is the "only smart contract supporting blockchain currently running in real-world production." The alliance is gaining traction, with the total number of members growing up to 186 as of May 2017.

Capital raising: token sales

Each blockchain and distributed application (both private and public) has a specific currency for conveying value, either called a token or a coin ("Token"), which is used to move data and/or pay transaction fees and computational services provided by the blockchain. By way of analogy, Tokens act similarly to an amusement park where tickets must be purchased to ride the attractions, as you must buy and use specific Tokens to pay for processing transactions on a particular blockchain. Bitcoin and Ether are the most well-known Tokens, each used as the currency on its respective blockchain.

Whereas an initial public offering ("IPO") is where shares of a company are offered to the general public for the first time, a token sale or initial coin offering ("Token Sale" or "ICO") is the offering of a portion of the initial supply of a Token to the public in exchange for legal tender or other cryptocurrencies, such as bitcoin or ether. As Alex Wilheim explained in an article for TechCrunch, "[a]n ICO is a fundraising tool that trades future cryptocoins in exchange for cryptocurrencies of immediate, liquid value. You give the ICO bitcoin or ethereum, and you get some of Billy's New Super Great Coin."[256] For early buyers, they are betting that the project for which they have purchased Tokens will be successful, and the value of the Tokens will appreciate.

In a Token Sale offered by the Bancor Foundation,

$153 million

was raised in just three hours

Token Sales have been very successful. From January 1, 2017 to July 26, 2017, blockchain entrepreneurs raised nearly $1.4 billion through Token Sales,[247] as compared with approximately $347 million raised through traditional venture capital funding during the same period.[258] On June 20, 2017, $95 million was raised through the sale of Tokens by Status for its browser, wallet and messaging app.[259] In another Token Sale offered by the Bancor Foundation, $153 million was raised in just three hours.[260] Not to be outdone, the Tezos blockchain project raised $232 million, and represents the largest fundraising effort by a blockchain-based company strictly through a Token Sale to date.[261] Following Tezos' record Token Sale, Filecoin raised $250 million, solely from accredited investors, through a Token Sale (approximately $198 million) and traditional venture capital ($52 million) from firms such as Andreessen Horowitz, Union Square Ventures, the Digital Currency Group, and Sequoia Capital.[262] Likely driven by the overwhelming success of Token Sales in 2017, Kik, a Canadian messaging app, announced plans for

a $125 million Token Sale of its "Kin" token, making Kik one of the highest-profile companies to hold such a sale. Kik's sale ended September 26, 2017, after raising $98 million ($50 million in pre-sale and $48 million in public sale), $27 million short of their goal.[263]

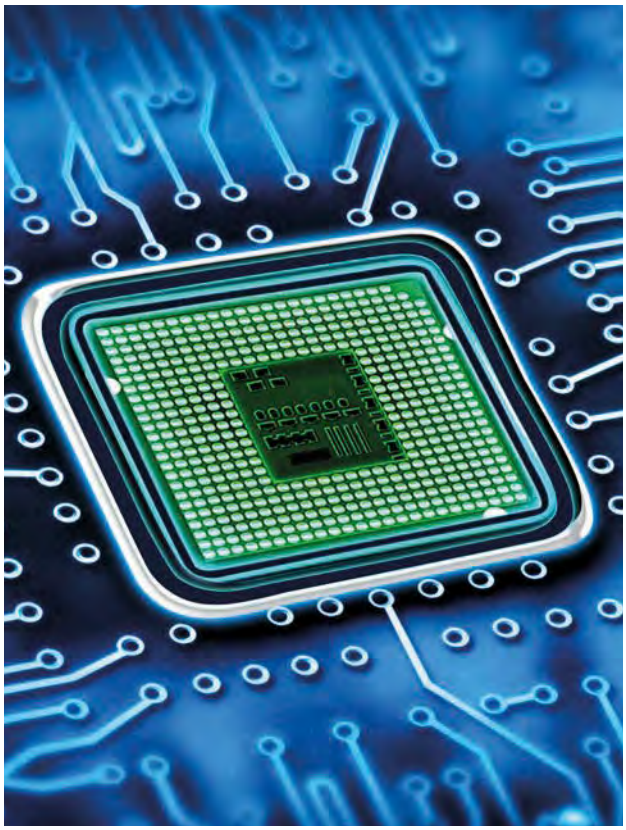
Companies are drawn to this method of fundraising because of its lower costs, lack of dilution, and perceived less-restrictive regulatory environment. Considering that, according to PWC, the average underwriter discount associated with an IPO is near 6.4 percent of the gross proceeds,[254] it's easy to see why a cheaper and potentially less regulated method for fundraising is desired. That being said, the uncertainty regarding a legal or regulatory framework creates its own set of risks.

It is also no longer individual retail investors buying Tokens. Established venture capital firms like the aforementioned Andreessen Horowitz, Sequoia, and Union Square Ventures are pouring millions of dollars into digital asset hedge funds. The total market value of all virtual currencies is currently past $160 billion,[255] up from just under $20 billion at the beginning of 2017. Bitcoin is up nearly 700 percent since 2016, and ether is up 3,300 percent over the same period. There are now more than 50 hedge funds dedicated to cryptocurrencies, with at least 15 in the process of forming. According to the hedge fund analysis firm Eurekahedge, from June 2013 through April 2017, the Eurekahedge Crypto-Currency Fund Index returned a cumulative of 2152.42 percent.[266] On an annualized basis, this comes to 125.45 percent for actively managed digital asset strategies, outperforming the Bitcoin Price Index by 103 percent.[267]

Token sale legal considerations

The lack of an established regulatory framework for Token Sales creates an uncertain legal path for those looking to hold a Token Sale. In fact, the process may be more complicated because of unique nature of each particular Token Sale, and the uniqueness of the characteristics and rights of each underlying Token. What a Token represents to a buyer is of critical importance in terms of potential legal issues and risks. When executed correctly, a Token Sale may be legally treated similarly to spot commodity transactions or non-equity based crowdfunding campaigns, like those done through Kickstarter or Indiegogo, but may also be a security. When execution is poor, the Token Sale may be subject to unintended scrutiny potentially from multiple regulators.

First and foremost, a company must understand the impact of their issuance of Tokens, the characteristics of the Tokens, how the Tokens are marketed or sold, and to whom and in which jurisdictions the Tokens are to be sold. Many Token Sales have been described as software pre-sales or currency sales, rather than public equity offerings, in a misguided attempt to escape regulatory burdens associated with securities. The Securities Exchange Commission ("SEC") has jurisdiction over "securities," as defined in section 21(a) of the Securities Act and section 3(a)(1) of the Exchange Act.[268] The term "security" includes, among other things, "investment contracts." "Investment



contract" is a prophylactic catch-all term that captures atypical products that function as devices for raising money.[269] The term is defined through case law as an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others.[270] This analysis is known as the "Howey Test." Securities may not be offered to persons unless the offeror has filed a valid registration statement with the SEC, or is relying on an exemption from registration.[271]

While there has been no case law yet with respect to Token Sales, in a Report of Investigation issued by the SEC on July 25, 2017 ("the SEC Report"), the SEC considered whether interests in an entity known as The DAO ("DAO Tokens") through the Ethereum network constituted an offering of securities.[272] The SEC explained that "U.S. federal securities law may apply to various activities, including distributed ledger technology, depending on the particular facts and circumstances, without regard to the form of the organization or technology used to effectuate a particular offer or sale."263 In order to qualify as an investment contract, the Tokens must satisfy each of the three prongs of the Howey Test: (1) that there is an investment of money; (2) that the investment is in a common enterprise; and (3) that the buyer of the Token expects profits for the efforts of others. If a Token fails one prong of the Howey Test, it will not be considered an investment contract from a federal securities law standpoint.

The SEC Report makes it clear that the SEC's review of Token Sales will be completed on a case-by-case basis, based on the facts and circumstances of each particular Token Sale, including the underlying rights of the buyers of the Tokens in such sales.

LabCFTC, a FinTech initiative of the CFTC, released a primer on virtual currencies that is intended to serve as an "educational tool" for market participants.[274] The primer covers the CFTC's jurisdiction over virtual currencies and tokens relative to the SEC, stating that "[t]here is no inconsistency between the SEC's analysis

and the CFTC's determination that virtual currencies are commodities and that virtual tokens may be commodities or derivatives contracts depending on the particular facts and circumstances."

If a Token would meet the relevant test to be treated as a security in a jurisdiction where preferred customers reside, the Token sellers should comply with relevant securities regulations or exemptions. In addition to being subject to securities laws, a Token Sale could be subject to review as a Ponzi scheme. A Ponzi scheme is an investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors, rather than from the returns of an underlying business activity. Many current Token Sales are based on white papers that outline the technical aspects of the underlying product and the problem it is intended to solve. That is to say, there is not always a proof of concept before the Token Sale. From a potential investors' perspective, the lack of a proof of concept when compounded with the ambiguous state of the law creates a situation ripe for fraud. From an issuer's perspective, an issuer must ensure there is a functional underlying business venture to create returns either prior to, or shortly after, the Token issuance. Issuers may also clearly outline the use of proceeds from the Token Sale to avoid the appearance of fraud. The uncertain and evolving Token Sale regulatory regime should encourage buyers and issuers alike to be cautious.

If a Token is found not to be a security at the federal level, it does not mean the Token or Token Sale escapes all securities law scrutiny. In the United States, without federal preemption, a Token may be subject to state blue sky laws (e.g., California's "Risk Capital Test"). Without a unified set of state laws dealing with the blockchain or cryptocurrencies, a state-by-state analysis must be completed to ensure a Token Sale is permissible and legal at the state level.

Furthermore, issuers in Token Sales must consider the applicability of other state and federal laws and regulations to their sales, including—from a tax standpoint—how to classify the proceeds of the sale, consumer protection laws, anti-money laundering laws, and financial terrorism laws. Issuers may also have to register as money transmitters with FinCEN, as discussed in the U.S. Regulatory Landscape chapter.

Other countries also have also begun to provide some clarity about the regulatory treatment of Token Sales. The Monetary Authority of Singapore (MAS) recently stated that it would consider certain Tokens as securities, depending on their underlying basis and the context of their issuance, a stance similar to that of the SEC.[275] Similarly, on September 9, 2017, the Financial Conduct Authority of the United Kingdom issued a similar "consumer warning" about the risks of Token Sales, including a statement that the determination of whether a Token Sale falls within its regulatory boundaries can only be decided on a case-by-case basis, depending on how such sale is structured.[276] Hong Kong's financial regulator, the Securities and Futures Commission (SFC), also announced that certain tokens sold in Token Sales may be classified as securities, and that digital asset exchanges may be subject to the SFC's licensing and conduct requirements.[277]

In June 2017, the chairman of the Australian Securities Investment Commission (ASIC) said that he would take a technologically neutral approach to ICOs, noting that they would be treated no different from issuings of more familiar financial instruments if

In addition to being subject to securities laws, a Token Sale could be subject to review as a Ponzi scheme.

they have the same characteristics.[278] Additionally, the Canadian Securities Administrators (CSA), a consortium of provincial securities regulators, published a report August 24, 2017, regarding "Cryptocurrency Offerings," finding that "many" of the Tokens investigated by regulators in Canada fall under the definition of a security, thereby triggering a range of legal requirements.[279] In an effort to better understand blockchain uses, the CSA had previously launched a FinTech "sandbox" aimed at jumpstarting FinTech projects that do not fit into the legacy regulatory framework (similar efforts have been launched in Singapore, Taiwan, and the UK).[280] More recently, Quebec's regulator for financial institutions, the Autorite des marches financiers (AMF), determined that a Token offered by Impak Finance was a security, but accepted the company into its regulatory sandbox, thereby relieving Impak Finance from certain requirements to which securities issuers would normally be subjected, including registration as a securities dealer and the requirement of a prospectus.[281]

In stark contrast to the actions of Canada, as discussed in the International Regulatory Landscape chapter above, China officially outlawed Token Sales on September 4, 2017, requiring all persons and organizations that had previously completed Token Sales to refund their investors.[282] South Korea has followed suit.

We expect other jurisdictions to continue to study Token Sales to determine the appropriate regulatory regime, and issuers should be aware of jurisdiction-specific requirements and risks, for where both the sellers and buyers will be located.

Without certainty regarding both the current and future legal environment for Token Sales, issuers will continue to face difficulties during the planning stages of such sales, and will need to perform increased due diligence prior to any sale.

Tokenizations

In addition, tokens can be used to create new investment products and digital representations of commodities or other financial products. For example, CME Group, in collaboration with The Royal Mint, is introducing a digitized gold offering called Royal Mint Gold (RMG), which will be a digital record of ownership for gold stored at the on-site bullion vault storage facility at The Royal Mint. The project will provide market participants with the opportunity to digitally trade physical gold via an electronic trading platform, using blockchain technology to record the ownership. These novel uses of tokens will raise a number of 'legal firsts' and new challenges, as regulators and trading participants evaluate issues such as title transfer timing, appropriate regulatory regime, license requirements, etc.

Potential risks

Although the blockchain has the potential to provide tremendous benefits to financial institutions and transacting parties more generally, widespread use of this technology does not come without risks and potential issues.

First, as with the implementation and adoption of any new technology across a space as complex and massive as the capital markets infrastructure, there are likely to be hiccups and growing pains along the way. It is difficult to predict the immediate impact that any glitches in blockchain adoption might have on individual transactions, or the future impact of those glitches on future adoption of the technology.

Second, some question whether the blockchain in its current technological state would be able to handle transactions in data classes with particularly high volume and speed requirements. Some analysts are skeptical as to whether the blockchain can be updated sufficiently frequently to be useful in such transactions. As a result of such skepticism, on August 1, 2017, the Bitcoin blockchain underwent a "hard fork" because of differences in opinions on how to effectively scale the blockchain's capacity to handle transactions. Upon the initiation of the hard fork, the Bitcoin blockchain was split into two separate and distinct blockchains, each with its own Token: (1) the original Bitcoin blockchain, and (2) the newly created Bitcoin Cash blockchain.[283] Prior to the

Bitcoin hard fork, the Ethereum blockchain underwent multiple hard forks. On July 20, 2016, the Ethereum blockchain executed a hard fork in order to return Tokens that were stolen in a hack related to the DAO Token Sale.[284] The Ethereum blockchain underwent three subsequent hard forks to resolve security issues that gave way to malicious network attacks.[285] While each hard fork was intended to resolve existing scaling and security issues, future hark forks will likely occur on the various blockchains as new security issues and scaling debates take place. Each such hard fork will bring with it a unique set of legal issues and considerations.

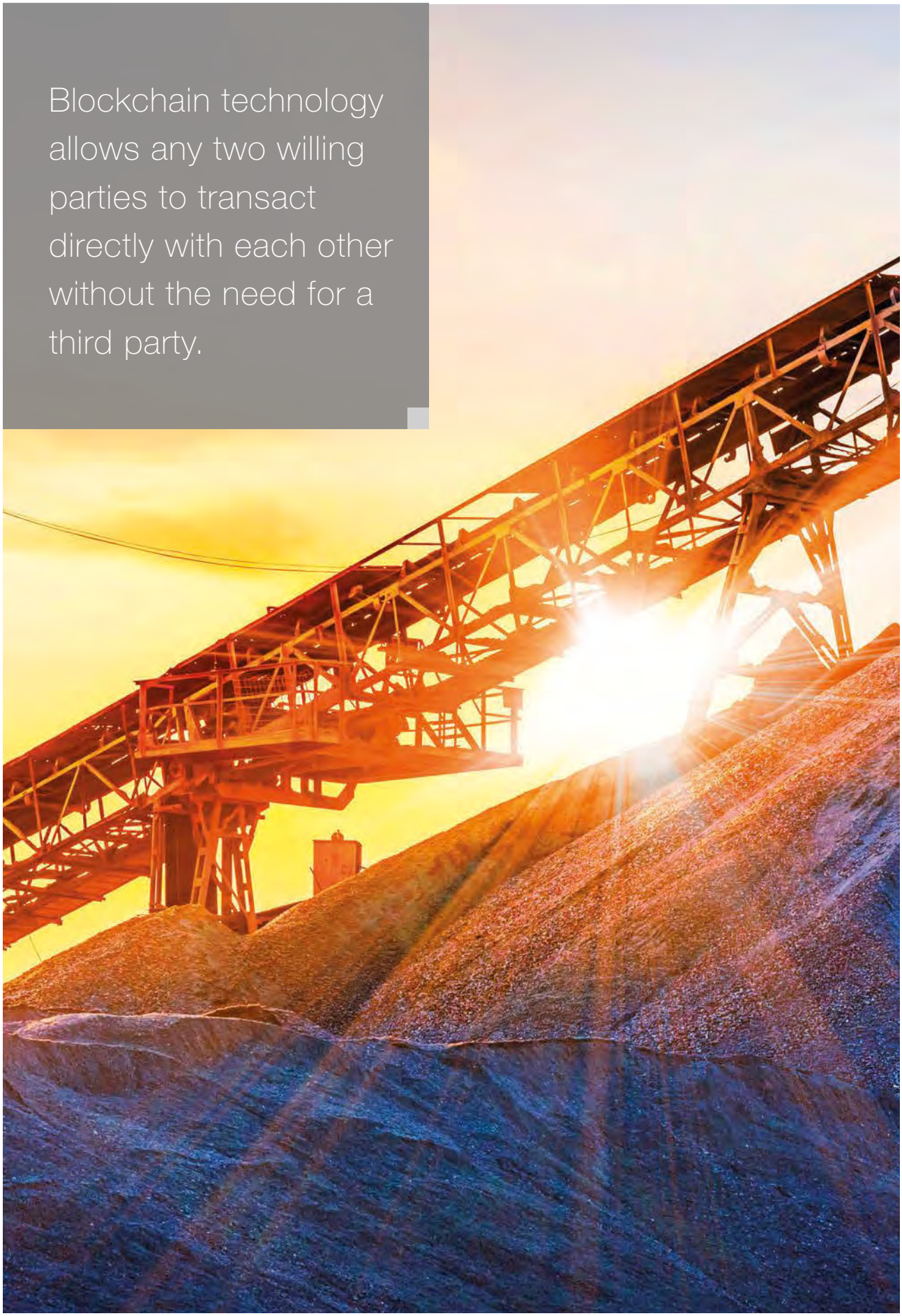
Third, as discussed elsewhere in this paper, there are numerous unanswered questions as to how regulators across the globe will react to the blockchain and virtual currencies more generally. Regulators are starting to become informed about these technologies, and soon will have a significant impact on the ability of financial institutions and other parties to implement blockchain technology into everyday financial transactions.

Finally, whether blockchain technology will impact capital markets will depend on the use of the technology by major financial institutions, and the extent to which these institutions develop the technology. Ironically, although cryptocurrencies were developed in the hope of reducing dependency on banks and other major financial institutions, whether these same institutions cooperate in instituting the technology will play a role in determining the impact that the blockchain has on capital markets.

Conclusion

Despite the potential downsides, the key attraction to blockchain technology for industry professionals is risk and cost reductions and efficiency. The blockchain offers the potential to improve the current infrastructure of financial transactions in significant ways: by making transactions more efficient and more secure, by providing more transparency and regulatory control, and by improving contractual performance. In addition to highly capitalized start-ups in this rapidly developing field, numerous major financial institutions have been spending significant resources on understanding and developing relevant applications, with increasing financial investment. We look forward to seeing what capital and technology developents 2018 will bring.

Blockchain technology allows any two willing parties to transact directly with each other without the need for a third party.



Blockchain innovation in the energy, commodities, shipping and trade finance industries

For the past few years at least, much of the water cooler conversation at financial services companies has focused on the impact that distributed ledger technology, or DLT, is having and will continue to have on the banking and payment industry.

However, the proliferation of blockchain technology has also sparked the conversation surrounding the impact of DLT on the energy and commodities sector.

On first glance, the convergence of the antiquated and long-established world[286] of crude containers, iron ore and grain on one hand, with nodes, hashes and algorithms on the other, appears to be a mismatched pairing. However—as outlined in this chapter—DLT is a natural fit in both the midstream and downstream sectors especially.

How will blockchain be useful?

First, many blockchain advocates argue that an immutable and self-executing record of the location and ownership should help to advance the traceability of many goods that, even today, remain susceptible to fraud and forgery. For example, a centralized record of ownership might have helped to allay some of the practical issues seen in the 2014 Qingdao metals fraud.[287]

The Natixis-, IBM- and Trafigura-pioneered DLT crude oil trading platform is an excellent example of this,[288] as the recording of trade confirmation through to delivery on a mutual digital ledger inevitably will help to mitigate the threat of tampering, misplaced records and unwanted litigation.

At the other end of the supply chain, the use of DLT and smart contract technology is allowing energy prosumers to maximize the economics of peer-peer energy trading. The well-known example of Brooklyn's solar microgrid,[289] in which local residents are able to trade excess energy on a decentralized market autonomously managed by a private blockchain, appears—on the face of it—to save time and cost, raise energy capacity, and even lower emissions. Whether this microgrid is a microcosm of the future of end-user energy trading remains to be seen. However, depending on both scalability and regulatory viability, the success of this model is a useful proof-of-concept for the nascent communion of blockchain and the energy market.

This section will explore and evaluate the potential application of DLT across a number of areas in the energy and commodity supply chain, including: (1) the

impact for producers and consumers; (2) energy trading; (3) trade finance; and (4) shipping, as well as the legal, commercial and regulatory impacts that blockchain may have on these industries.

Can it work?

When electronic trading and recording was introduced, many were skeptical as to whether the industry could thrive away from paper and the pits. Today, the complex power, gas, emissions, oil, metals and agricultural markets could not survive without the capability of the internet. It will not be surprising if, much like electronic trading, blockchain's application to this sector quickly turns to one of widespread acceptance and ultimately, dependence.

Energy producers and consumers

Blockchain technology allows any two willing parties to transact directly with each other without the need for a third party. How might this apply to the energy industry?

At a broad level, an autonomous distributed ledger in which transactions are executed directly between producers and consumers has the potential to decentralize the often-rigid energy eco-system, empowering end-users in the process.

Peer-peer trading

One example is the Australian company Power Ledger, which has built a peer-to-peer energy trading application that allows asset owners to monetize surplus energy generation, without the need for an intermediary such as the grid. Instead, Power Ledger's blockchain-based system has the ability to track input and output of energy (in this case, solar), and validate trade-settlement based on standard terms and conditions, which are executed using smart contract code.[290]

Of course, many of the complex and intricate regulations that underpin national power markets, for example, the UK's Balancing & Settlement Code,281 do not contemplate mass decentralization. In addition, a system that relies on the sharing of potentially sensitive transaction data, will need to balance the need for transparency against the requirement to comply with any applicable data protection laws. Despite the obvious uplift, there is precedent for energy systems adapting to market changes. For example, as distributed generation has increased in recent years, the UK national grid has been forced to modernize a linear flow-system into one that is capable of dealing with reverse flows.

Whether blockchain's empowerment of the prosumer can evolve from closed-use cases to a true revolution will depend heavily on regulatory engagement. However, as the increase in renewable energy inputs from decentralized sources disrupts the traditional energy system,282 it appears to be an apt time for the industry to embrace blockchain technology.

Asset registration

Many of us will likely have been through the tiresome process of switching energy providers. The UK's Office of Gas and Electricity Markets (OFGEM) has recently published data that shows that the average gas and electric switching time in the UK is 16 days.[293] In an economy where many far more complex transactions can be effected at the click of a button, this appears to be somewhat archaic.

OFGEM has recognized this and has since committed to delivering next-day switching by 2019.[294] This commitment would require the coordination of all UK power and gas suppliers' meter databases. Holding this deluge of information in one centralized system would be at best costly and at worst unmanageable.

A blockchain-based decentralized meter registration platform, such as that being piloted by the UK start-up Electron on the Ethereum blockchain,[295] may very well help OFGEM (and similar national bodies) to achieve this goal. Taking this one step further, smart contract code might allow consumers to shift across a multitude of suppliers over the course of a day, taking advantage of the best price at any given time, with the blockchain producing a consolidated statement at the end of the day.

In short, one of the fundamental principles of blockchain—namely the ability to store data on a

decentralized system that is independent from a central authority—would help to directly link consumers, producers and their respective assets, simplifying the multi-layered energy ecosystem we see today.

The ability to record energy assets on shared blockchains would also allow energy regulators to easily monitor capacity and performance of power-stations, facilitating market participants' compliance with reporting legislation, such as the European powers and gas regulation, REMIT.[296]

Licensing and liability

DLT allows for direct contractual relationships to be established between energy prosumers, each of which may act as a "supplier" to another in a closed network at any time. In many jurisdictions, this activity would normally require the supplier to obtain a license from the necessary regulatory authority. Depending on the number of prosumers in each network, this may be unmanageable. Regulators will therefore need to evaluate the system to ensure it can trust the veracity of the blockchain in order to waive such stringent requirements, which again will likely involve protracted dialogue.

Further, the potential removal of a central authority from the supply chain would leave key commercial questions surrounding liability for operational failure, settlement and payment defaults (to name a few), up in the air. Perhaps adherence to a standard set of terms and conditions, with certain conditional logic triggers for these eventualities,[297] might help to fairly and effectively apportion liability in the event of counterparty default.

Conclusion

While blockchain may at first appear to be a form of technological disruption that the traditional energy ecosystem may be inclined to resist, it could become the foundation of new decentralized markets. If the above-mentioned pilot schemes prove scalable, DLT may catalyze the evolution of a market where businesses and homes consume, produce and trade energy in a transparent and efficient manner. [298]

Energy trading

The energy trading markets are perhaps one of the best-suited arenas for the integration of blockchain technology. Oil and natural gas are two of the most actively traded commodities—and they are also some of the most difficult to deliver and store. Moreover, current technology does not allow sufficient quantities of electric power to be stored on a battery, and therefore the resource must typically be used upon delivery or transferred. The development of digital assets backed by physical energy resources could monetize reserves of oil and gas resources lying dormant in storage facilities, provide a virtual storage mechanism for electric power, and make these products highly liquid. Energy derivative transactions may also in the future be executed and cleared instantaneously through blockchain-based platforms. Blockchain technology could facilitate compliance with U.S. and international regulatory recordkeeping and reporting requirements associated with such transactions.

Commodity-backed tokens

Oil and gas held in storage facilities and electric power-generating capacity may be tokenized and traded. One example of a commodity-backed token is bilur.[299] This token is marketed as a vehicle for "bringing the energy market to the people." It is backed by units of stored energy. The value of bilur is calculated daily with Standard & Poor's Platts Dated Brent assessment. 1 bilur is equivalent to 1 Ton Oil Equivalent (TOE) of Brent crude or 11.6 MWh of energy. It is issued on a private Ethereum network and may be traded among individuals or on an organized digital asset exchange.

Energy trading platforms

Energy products may also in the future be traded on decentralized orderbooks relying on blockchain technology. A consortium of European energy trading firms is working to develop such a platform, called Enerchain, that would allow peer-to-peer trading of wholesale energy market products.[300] The platform would offer day-ahead, monthly, quarterly and yearly baseload for power and gas. The project is in the proof-of-concept phase, which concludes at the end of 2017.

Blockchain may also facilitate peer-to-peer energy trading among persons and companies that generate electricity through solar panels or other means. However, current U.S. energy laws and regulations would likely pose a barrier to the development of such a market. Accordingly, many of these initiatives are in the works overseas.[301]

Physical energy transactions

Companies are developing blockchain technologies to streamline physical commodity transactions. Commodity trading house Mercuria and the banks ING and Société Générale are working toward executing a large oil transaction using a blockchain.[302] The parties envision that the technology will reduce the amount of paperwork required for title to pass from buyer to shipper to seller.

Commodity trading firm Trafigura and French bank Natixis are exploring the use of blockchain technology to facilitate physical crude oil transactions.[303] They hope to offer a distributed ledger that all parties to a transaction can input documents onto and simultaneously view at all stages of the transaction.

Derivative transactions

Energy derivatives are very popular hedging instruments for commercial businesses and are frequently traded by speculators. Blockchain technology has the potential to disrupt how these instruments are typically executed and cleared.

The International Swaps and Derivatives Association ("ISDA") recently issued a white paper analyzing the merits of trading swaps through blockchain technology, as discussed above.[304] The whitepaper proposes the use of a blockchain to store electronic ISDA Master Agreements. The agreements would contain conditional logic triggers programmed by smart contract code, which would facilitate the automation of certain provisions within swaps documentation. This could also apply to energy transactions executed subject to ISDA Master Agreements that include one or more of the ISDA energy product Annexes.

Moving ISDA documentation to the blockchain could facilitate automated compliance with both the CFTC swap data reporting and margin requirements in the United States, and EMIR reporting requirements in the EU.[305] The blockchain might feed swap data directly into a swap data repository as events occur in real time, or eliminate the need for these institutions altogether. Moreover, the exchange of margin could be streamlined and automated using blockchain, smart contracts, and third-party data feeds, known as "oracles." Day-to-day compliance with the regulations could theoretically be embedded into smart contracts. For example, bank accounts or digital currency wallets could be linked to the smart contract and automatically exchange variation margin as required. Similarly, the smart contract could be designed to automatically submit swap continuation data and other reports to a swap data repository upon the occurrence of a life cycle event, providing regulators with direct and unencumbered access. Moreover, counterparties would have all of their

swap documentation and confirmations stored on the permissioned, private distributed ledger, reducing the volume of records required to be maintained. This would make it much easier for swap counterparties to comply with some of the more onerous requirements imposed by the Dodd-Frank Act, for example.

Shipping

In a world where 90 percent of goods in global trade are carried by ships, and shipping transactions often involve dozens of people and organizations, generating more than 200 different interactions and communications among them,[306] it is not surprising that the shipping industry is increasingly looking to blockchain to streamline global supply processes, improve transparency and protect against fraud.

Yet having been at the heart of international commerce for centuries, it is also an industry steeped in tradition that has historically been slow to embrace change. This chapter considers how new blockchain technology could transform the global shipping industry through the development of digitized supply chains, electronic bills of lading, marine insurance platforms, and smart contracts, and discusses the prospects for industry's adoption of this technology.

Digitized supply chain

The shipping industry is paper-intensive. Most shipping transactions involve sales contracts, charter party agreements, bills of lading, certificates of origin, port documents, letters of credit and many other documents related to a vessel and its cargo.[307] Traditionally, these documents were passed physically between multiple parties spread across the globe. The internet now, of course, facilitates the digital exchange of documents, but this occurs bilaterally and therefore still causes delays along the supply chain.

Moreover, 80 percent of shipping documentation is still in paper form.[308] Conversely, parties along the shipping supply chain using blockchain technology would be able to upload and share documents instantaneously and securely. This would allow every participant to track and manage the shipment's progress and documentation from end to end, increasing efficiency and transparency, while simultaneously reducing costs and the risk of documents being delayed, misplaced or tampered with.[309] By storing and securing in real-time all information related to a transaction, the blockchain reduces not only the risk of fraud and data loss, but also the need for a paper trail.

With such a large proportion of shipping documentation in paper form, it is estimated that going paperless could save up to US$300 per container.[310] It is easy then to see why paperless supply chains are hugely appealing to the industry. Industry giants Maersk and IT are leading the way, having combined their significant resources to develop a new product that aims to create a fully digitized supply chain. Meanwhile, South Korean liner operator Hyundai Merchant Marine recently announced completion of its first pilot voyage as part of a South Korean consortium comprising 15 members, including Amazon Web Services, Korea Customs Service, Busan Port Authority, Namsung Shipping, Microsoft, and Samsung. The pilot voyage tested the feasibility of combining blockchain technology with the Internet of Things technology ("IoT"), to achieve real-time monitoring and managing of reefer containers during the pilot voyage.[311]

Other companies are experimenting with blockchain supply chain management tools. For example, a group of food companies, including Walmart and Dole, are working with IBM to develop DLT supply chain solutions.[312] They hope to use DLT to maintain records of and track inventory. The new technology might also help them quickly pull contaminated products from the supply chain.

Providing shippers, freight forwarders, ocean carriers, Customs authorities and other relevant parties the ability to access a complete set of constantly updating documents would, in addition to reducing inefficiencies, allow parties to amend the transaction according to how it proceeds. For example, upon learning from one node in the supply chain of an obstacle or delay, the buyer and

the seller might decide to modify the contract's quantity in order to adjust to the change in circumstances. This would be a welcome improvement for an industry where flexibility is highly valued.

Electronic bills of lading

As we highlighted in our client alert last year, electronic bills of lading ("e-bills") are not a new concept.[313] Indeed, the International Group of P&I Clubs has approved three electronic trading systems ("ETS") on which e-bills can be created and traded.

Yet the industry has been slow to depart from paper bills. This is in part because of uncertainty as to whether e-bills can comprehensively mirror and replicate the highly evolved and complex legal framework for paper bills of lading.

While ETS's seek to replicate the existing framework through user agreements, the extent to which courts in foreign jurisdictions will recognize such user agreements and accept e-bills is yet to be tested. Blockchain technology could make the legal distinction between paper and e-bills less problematic. The technology guarantees that each e-bill is and remains entirely unique. This ensures that only the holder of the e-bill can exercise the right to claim the goods, making blockchain e-bills better suited to use as a document of title than traditional e-bills.

Another common concern with e-bills is hacking. While paper bills have historically been open to being altered, switched and otherwise tampered with during their lifecycle, e-bills created on centralized ETS such as Bolero are equally vulnerable to cyberattacks, a threat that is not covered by P&I cover. Blockchain mitigates this risk by de-centralizing the system and making it significantly harder to hack. Indeed, in the wake of the recent cyberattack on Maersk, estimated to have cost between US$200 and US$300 million, industry commentators have noted that blockchain technology could have helped to prevent the attack.[314]

Marine insurance

EY, in collaboration with AP Moller-Maersk, Microsoft and Guardtime (a data security provider) announced plans to launch the world's first blockchain platform for marine insurance. Innovation in this space is long overdue, according to Lars Henneberg, head of risk and compliance at AP Moller-Maersk.[315] The platform, set to go live in 2018, has the potential to revolutionize one of the oldest branches of insurance in the world. Marine insurance is historically a cumbersome, paper-heavy industry, and estimates are that the new platform could significantly reduce paperwork, delays and disputes in the US$30 billion marine insurance market.[316]

The platform will allow insurers, insureds, brokers and third parties to input data about identity, risk and exposure in distributed ledgers; link this information to individual insurance contracts; and make payments via bitcoin.[317] The result, it is hoped, will be faster billing and collection, greater clarity on claims histories, more accurate exposure management, and improved compliance.

Smart contracts

The major breakthrough offered by blockchain technology, other than its function as a public ledger that securely stores and updates information in real-time, is the "smart contract."308 As described above, a smart contract is an agreement written in computer code to automatically execute the contract's terms when its conditions are met.[319] Counterparties to a smart contract would negotiate the major terms, such as product specification, quantity, price, and timing and location of delivery, through the blockchain in a process most closely analogous to negotiating a derivative contract over an electronic over-the-counter exchange. In addition to increasing the speed of a contract's execution (authorizations for port clearance, ship departure or wire transfer would occur immediately upon the satisfaction of pre-set conditions, rather than upon the counter-party's notice of satisfaction of those conditions), the self-executing nature of smart contracts reduces the risk of non-compliance. The obligor in a smart contract loses the ability to withhold payment because payments occur automatically through the blockchain.

The automatic nature of the smart contract also creates limitations. If the obligor's smart contract-linked account had no remaining funds, the lender might not necessarily want the smart contract to automatically initiate the default process.[320] Similarly, some other change of circumstance, such as an impending military conflict or a natural disaster, may clearly signal to human minds the need for a contract modification, but may not be interpreted correctly (or picked up at all) by the algorithms used by smart contracts. While it is foreseeable that blockchain technology and the smart contracts afforded by it will become increasingly sophisticated over time, there may be no substitute for human judgment, and therefore an inherent limitation on the usefulness of smart contracts in this sector.[321] Please see the Smart Contracts chapter above for additional information about this technology.

Prospects for adoption

Enhancements in efficiency, speed and data security of shipping transactions that would come from widespread adoption of blockchain technology are some of the chief forces generating enthusiasm for blockchain among shipping players.

The blockchain, given its role as a system, is also ripe to be combined with other promising technologies. For example, IoT is beginning to be tested in conjunction with blockchain technology. IoT is a way of connecting physical objects with the digital world. The shipping industry is thus particularly interested in this technology.

If the goods in shipments were able to be individually tracked—as IoT hopes to accomplish—then there would be a drastic increase in supply awareness and a decrease in fraud. For example, most goods shipped en masse end up getting mixed in with each other on long journeys, and are thus difficult to distinguish. This state of affairs results in compromised quality and, in some instances, accusations of fraud. But if every avocado shipped from Mexico to the Far East wore a barcode that scanned into the blockchain at all nodes on the supply chain, it would be easy to determine which were the rotten avocados that infected the rest of the

shipment and, most importantly who shipped those avocados (or who placed horse apples in containers labeled as avocados).

The blockchain would thus know which party was in breach, and if a smart contract was used, it would automatically respond in accordance with the terms of the contract. However, as indicated above, the automation that is foundational to smart contracts could also frustrate successful implementation of a shipping transaction, and thus deter its widespread adoption.

Furthermore, the human element can corrupt the data that the blockchain relies upon. If a port employee tasked with scanning avocados was bribed to make false inputs, then the data that the blockchain was expertly storing and securing upon would be false. Blockchain will likely rely heavily on the Global Positioning System (GPS), but GPS can—and has—been manipulated by hackers. A chain is only as strong as its weakest link, and for blockchain technology, the weakest link might be the one where the digital world meets the physical one.

Trade finance

In the past few years, there has been a significant increase in banks' interest in the development and use of blockchain technology in the context of trade finance operations. This is not surprising—a data structure that can streamline the financing process, which

currently remains largely paper-based, expensive and complicated, appears to be long overdue.

Blockchain promises to reduce time required for the completion of transactions and associated costs, while increasing transparency between the participants and mitigating fraud risks.

First transaction – Barclays and Wave

In 2016, Barclays and Wave, an innovative start-up company, executed the first global trade transaction using distributed ledger technology.[322] The platform developed by Wave, where trade documentation was processed with funds remitted via Swift, facilitated the letter of credit transaction between Ornua and Seychelles Trading Company.

The technology established by Wave aims to negate the inefficiencies inherent in trade finance. Trade transactions usually involve a number of participants who are often located in different jurisdictions, and a large volume of paperwork that needs to be approved, countersigned by and delivered to various parties. Wave, however, has developed a system that allows all relevant participants to transfer title, and view and transmit shipping documents through a secure decentralized network.

As a result, the transactions take less time to complete—the deal between Ornua and the Seychelles Trading Company only took four hours—compared with seven to 10 days that this process would have taken if carried out conventionally.

In January 2017, Deutsche Bank, HSBC, KBC, Natixis, Rabobank, Société Générale and UniCredit made a decision to cooperate to develop and commercialize aDigital Trade Chain consortium, the aim of which is to simplify trade finance for businesses.[323] The banks involved IBM as a party to assist with production of such system.[324]

Advantages of blockchain in trade finance context

In addition to increasing time-efficiency, the related costs are substantially reduced. Barclays in particular identified direct savings with the courier services that the Wave platform does not require. More generally, since around 5 percent of the costs in trade transaction arise from dealing with documentation, deploying blockchain systems would facilitate a move to paperless trade, error-free documentation and fast transfer of originals.[325] Blockchain is updated quickly by each member on the network, and shows the most recent transactions, meaning there is no need for multiple copies of the same document to be stored on various databases by different parties.

A blockchain platform where all transactional detail would be logged and stored on an immutable, shareable, digital ledger is also seen as a reliable way to stop documentary fraud.[326] It provides necessary visibility throughout the supply chain: parties can track vessels, commodities, sign approvals, store documents and make payments.

A single blockchain can summarize all of the necessary information in one digital document, which can be reviewed by all participants at the same time, and is updated almost in real time.[327] The technology also has the potential for utilization of capital that would otherwise be locked up while being disputed or waiting to be transferred between parties in the transaction.[328]

Letters of credit – a blockchain revolution?

As mentioned earlier, the transaction executed by Wave and Barclays concerned a letter of credit as a financing mechanism.

Letters of credit have been used by the trading industries for centuries, and the principle underpinning their operation has barely changed throughout the time.

In modern practice, when a company in one jurisdiction seeks to import a shipment of goods from a supplier based overseas, it bears risks related to payment to the supplier before making sure that the goods will arrive as ordered. The exporter is also exposed to uncertainty as to whether it is going to be paid, so ordinarily would not ship the goods without some assurance. To solve this problem, the importer's bank, which issues a letter of credit, promises to pay the exporter's bank once certain documents have been

provided by the exporter. These documents should be in strict compliance with the requirements, and are designed to prove that the goods have been loaded onto the vessel (or other mode of transport). In this scenario, the banks hold the money for the buyer and the seller, who are now protected.

This structure contemplates a very substantial amount of paperwork that needs to be circulated between and approved by all four parties involved, together with shipping companies and agents, insurers and others.

A prototype developed by Bank of America Merrill Lynch, HSBC and the Infocomm Development Authority of Singapore is designed to simplify paper-heavy letter-of-credit transactions.[329]

The trade deal can be executed automatically through a series of digital smart contracts, as explained in the Smart Contracts chapter above. The members on the network can access data almost instantly after it has been added or modified, and can see the next steps that need to be taken.

The seven steps to a blockchain-based letter of credit transaction are:

- The importer creates a letter of credit application for the importer bank to review and stores it on the blockchain.
- The importer bank receives notification to review the letter of credit and can approve or reject it based on the information provided. Once checked and approved, access is then provided to the exporter bank automatically for approval.
- The exporter bank approves or rejects the letter of credit. If approved, the exporter can see the letter of credit requirements.
- The exporter completes the shipment, adds invoice and export application data, and attaches a photo image of any other required documents. Once validated, these documents are stored on the blockchain.
- The documents are reviewed by the exporter bank, which approves or rejects the application.
- The importer bank reviews the data and images against the letter of credit requirements, marking any discrepancies for review by the importer. When approved, the letter of credit goes straight to completed status or is sent to the importer for settlement.
- The importer can review the export documents and approve or reject them, if required.[330]

SMEs

The other advantage of blockchain is that it allows SMEs to access trade finance. Utilizing blockchain applications, an SME would be able to receive funding at a lower cost compared with traditional forms of financing. It is envisaged that the banks will vet SMEs before adding them to the platform.

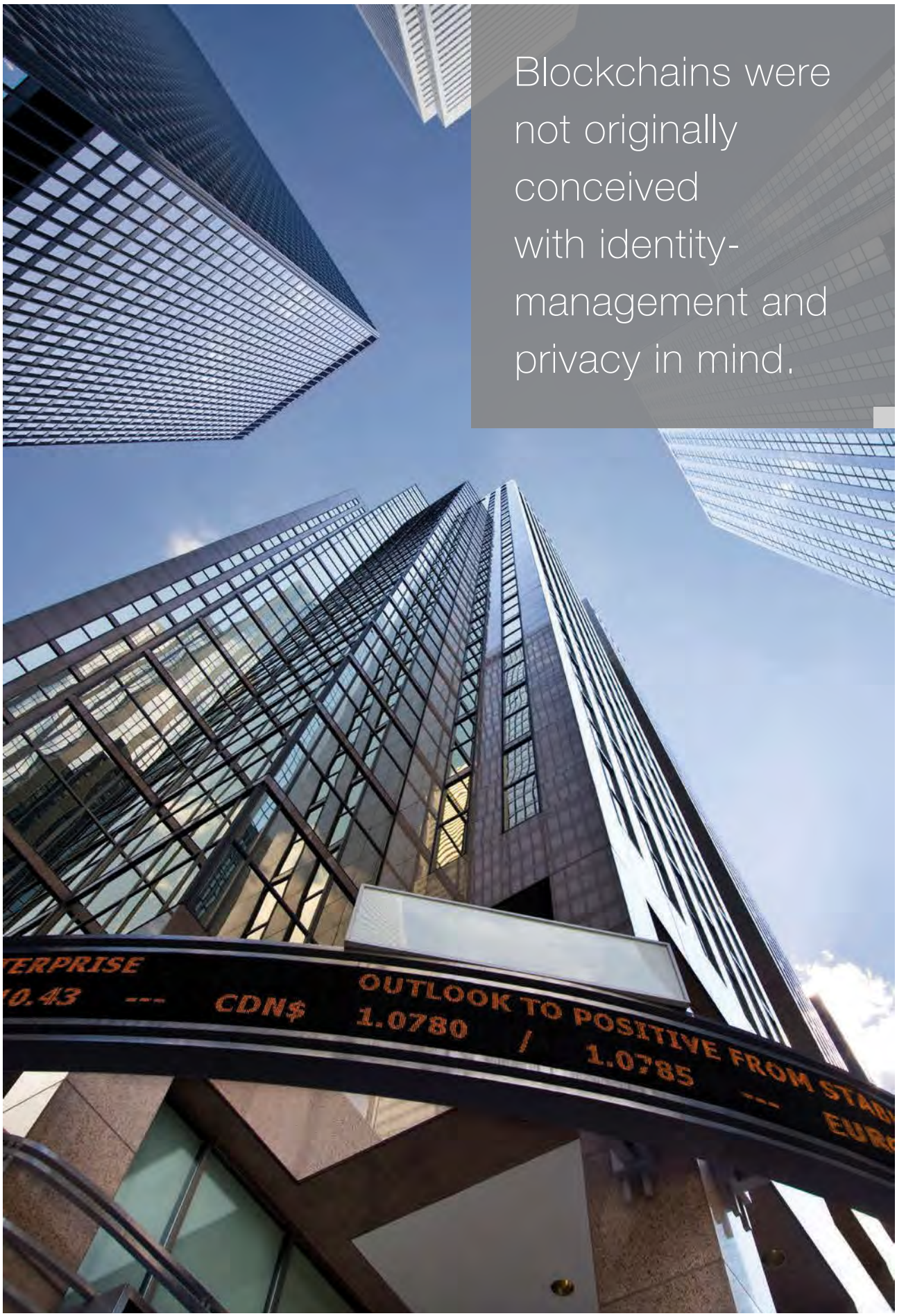
There are more than 20 million SMEs in Europe, for example, providing around 85 percent of jobs[331] and contributing up to 40 percent of national income. However, approximately 50 percent of SMEs do not have access to formal credit. Use of blockchain technology would, no doubt, positively affect growth in the SME sector.

Legal uncertainty?

One of the key legal issues related to the operation of blockchain-based projects arises out of the cross-jurisdictional nature of trade finance deals. Since systems are decentralized, it can be difficult to establish where a breach or other omission has occurred.

Legal enforceability of smart contracts is another concern, as we analyze in the Smart Contracts section above. Such would argue that smart contracts may lack the familiar contractual concepts such as offer, acceptance, consideration, etc.

However, there are numerous solutions to the above potential problems that would depend on the precise nature of the deal, which could be reflected in drafting agreements governing the relationships between the participants. Much in this sector will come to depend upon platform rules, or umbrella agreements, governing transactions or the platform requirements.


Blockchains were not originally conceived with identity-management and privacy in mind.
ERPRISE
0.43 --- CDN$ 1.0780 / 1.0785 ---
OUTLOOK TO POSITIVE FROM STA

Privacy and re-identification on the blockchain

As one paper noted, "anonymous digital cash is another state-of-the-art technology for Internet privacy. As many observers have stressed, electronic commerce will be a driving force for the future of the Internet. Therefore, the emergence of digital commerce solutions with privacy and anonymity protection is very valuable…"[332] Since the paper in question, "Privacy-enhancing technologies for the Internet" was published in 1997, the authors thought not of Bitcoin but of a predecessor, DigiCash's ecash. However, the paper identified risks to privacy in using anonymous digital cash that have only grown:

> Of course, the DigiCash protocols only prevent your identity from being revealed by the protocols themselves: if you send the merchant a delivery address for physical merchandise, he will clearly be able to identify you. Similarly, if you pay using ecash over a non-anonymized IP connection, the merchant will be able to deduce your IP address. This demonstrates the need for a general-purpose infrastructure for anonymous IP traffic… In any case, security is only as strong as the weakest link in the chain.[333]

Bitcoin has been described as "anonymous but not private: identities are nowhere recorded in the Bitcoin protocol itself, but every transaction performed with bitcoin is visible on the distributed electronic public ledger known as the block chain."[334] In addition, an individual Bitcoin user may use one (or very many) public keys (sometimes referred to as a "bitcoin address") to engage in transactions. These public keys do not identify individual users, and without additional data or analysis, one cannot determine whether two (or more) public keys are linked to the same user. Therefore, the Bitcoin protocol theoretically provides for anonymity (but not privacy) in transactions because the blockchain does not involve recording any identifying information to individual public keys.

Privacy

In the wake of major breaches of traditional, centralized databases containing personally identifiable information

masking network participants on the public ledger increases the complication of implementing know-your-customer and anti-money laundering measures.

("PII"), the notion of a decentralized framework for managing identity on the blockchain could actually increase privacy protection in the long run by giving more agency over PII to individuals. Re-distributing and decentralizing these data points could have the advantage of "limit[ing] and control[ing] how much information you share while retaining the ability to transact" rather than having to provide a wealth of personal information up-front to a trusted third-party intermediary to engender trust and ensure accuracy.[335]

However, there are key distinctions between anonymity and privacy, and in practice, it may be difficult to maintain both when using Bitcoin or other blockchain-based applications. Blockchains were not originally conceived with identity-management and privacy in mind. In fact, some chinks in the armor of privacy when using Bitcoin and other blockchain applications are akin to those described 22 years earlier as to DigiCash. Some blockchain application users voluntarily disclose their public keys; in so doing, they may either intentionally or unintentionally allow others to link identifying data with these public keys. Those who are able to link public keys with this outside identifying information may have the ability to then analyze the blockchain and potentially determine the identity of the user. This identifying data does not necessarily have to be as specific as a person's name, address, or phone number. It could be something as seemingly innocuous as the knowledge that a particular user made a purchase with a particular business around a certain time.

For example, at the onset, many users purchase digital currency through an online wallet or exchange service. That wallet or exchange service has the personal information of the purchaser. Digital currencies for these users are effectively no more anonymous than a bank account, although this loss of anonymity takes place at the point of entry into the currency and is not a feature of the blockchain protocol itself.

Further, some users voluntarily reveal or disclose their public keys, whether publicly (as may be the case for businesses accepting digital currencies as payment), or through blockchain.info, or more privately in forums or signature lines in internet posts. In this respect, one may think of a blockchain application public key in a way similar to an email address: some email addresses may be relatively anonymous in nature (for example, an email that does not reveal one's name or initials), but one may of course still choose to reveal that email address to acquaintances.

In addition, "[e]ven supposing one manages to acquire bitcoins without giving up personal information, one's real-world identity can still be discovered in the course of transacting bitcoin within the network."[336] As discussed above, when outside information becomes linked with a particular public key, there is a risk that re-identification may occur through various types of behavior-based clustering analysis of the blockchain, and in some cases, analysis of the IP addresses of nodes adding blocks to the blockchain.

In the case of Bitcoin and other digital currencies, there is not only the risk that a delivery order to a physical address will lead to re-identification, but there is also, in the distributed ledger itself, a large amount of public data on transactions made with the digital currency, leading one author to note:

> A complementary source of potentially deanonymizing information is available to every computer that participates in the decentralized transaction network by hosting a bitcoin node. This information is the set of IP addresses of the computers that announce new bitcoin transactions…

An example of this kind of IP address deanonymization made public is blockchain.info, which discloses the IP address of the first node to report a transaction to its servers. The information is only as reliable as the web site's node connectivity: with a declared 800–900 connected nodes at the time of writing, it is probably not enough to reliably pinpoint the originating IP in all cases.[337]

The process of recording and managing sensitive information on blockchains requires special attention, given that "the distributed nodes element of the technology" creates "increased attack surface (every node has a copy of everything)," potentially increasing the visibility of private information, as well as the security risk of unauthorized distribution of that data.[338] Some developers have designed around the availability of participant and transaction information on the blockchain to add additional layers of privacy. For example, Zcash uses a 'zero-knowledge proof algorithm to verify transactions without the need to disclose the identity of participants or the amount of each transaction.[339] While this can help prevent re-identification, the approach of masking network participants on the public ledger increases the complication of implementing know-your-customer and anti-money laundering measures.

Psyeudonymity concerns

Some of the concerns surrounding the privacy and pseudonymity on the blockchain are similar to the concerns of pseudonymity raised in other industries and other contexts. For example, the National Institute for Standards and Technology ("NIST") has issued standards regarding pseudonymity and deidentification. The NIST standards concern a different type of pseudonymity issue than is present in blockchain applications. Specifically, the NIST standards concern data sets that have been stripped from PII, and the risk of re-identification from those data sets. These standards are aimed at companies managing individuals' sensitive information so as to not inadvertently reveal their identities. In contrast, the "rules of the game" concerning pseudonymity on the blockchain are more well-known and "spelled out." Further, Bitcoin users have more control over whether they may be re-identified, and can take various actions to greater maintain privacy (however, this increased privacy may lead to higher transaction costs). NIST defines pseudonymization as a "specific kind of de-identification in which the direct identifiers [like names or account numbers] are replaced with pseudonyms."[340] NIST defines "re-identification risk" as "the measure of the risk that the identities and other information about individuals in the data set will be learned from the de-identified data."[341] The factors that determine re-identification risk include: "the technical skill of the data intruder, the intruder's available resources, and the availability of additional data that can be linked with the de-identified data."[342]

The report includes a number of highly public instances in which pseudonymized identities were re-identified based on ancillary information, from movie choices to medical outcomes to location data.[343] However, as NIST warns, "In many cases the risk of re-identification will increase over time as techniques improve and more background information become available."334 In the case of distributed ledger technology, the permanence of transaction history ensures that the transaction history available to analyze continues to expand even as the techniques to do so improve over time. NIST's concern regarding re-identification risk is mirrored internationally. For example, under European privacy law, a pseudonym is personal data under specific standards set forth by the Article 29 Working Group. [345] "Pseudonymity is likely to allow for identifiability, and therefore stays inside the

scope of the legal regime of data protection."[346] The Article 29 Working Group lists as a "common mistake":

> Believing that a pseudonymized dataset is anonymized….Many examples have shown that this is not the case; simply altering the ID does not prevent someone from identifying a data subject if quasi-identifiers remain in the dataset, or if the values of other attributes are still capable of identifying an individual.[347]

The paper identifies as weaknesses of the pseudonymous approach, "the user using the same key in different databases," as well as storing the key to re-identify in the same place as less secure data. "If the secret key is stored alongside the pseudonymized data, and the data are compromised, then the attacker may be able to trivially link the pseudonymized data to their original attribute."[348] And whether or not it is pseudonymized, the immutability and permanency of information on a block in a blockchain could conflict with the "right to be forgotten" under European privacy law.[349]

Pseudonymization is a key concern to big data generally, and is at the forefront of a number of industries that are currently grappling with the potential for blockchain to revolutionize the potential privacy risks inherent in the high levels of transparency of blockchain technologies.

Industry-specific privacy concerns

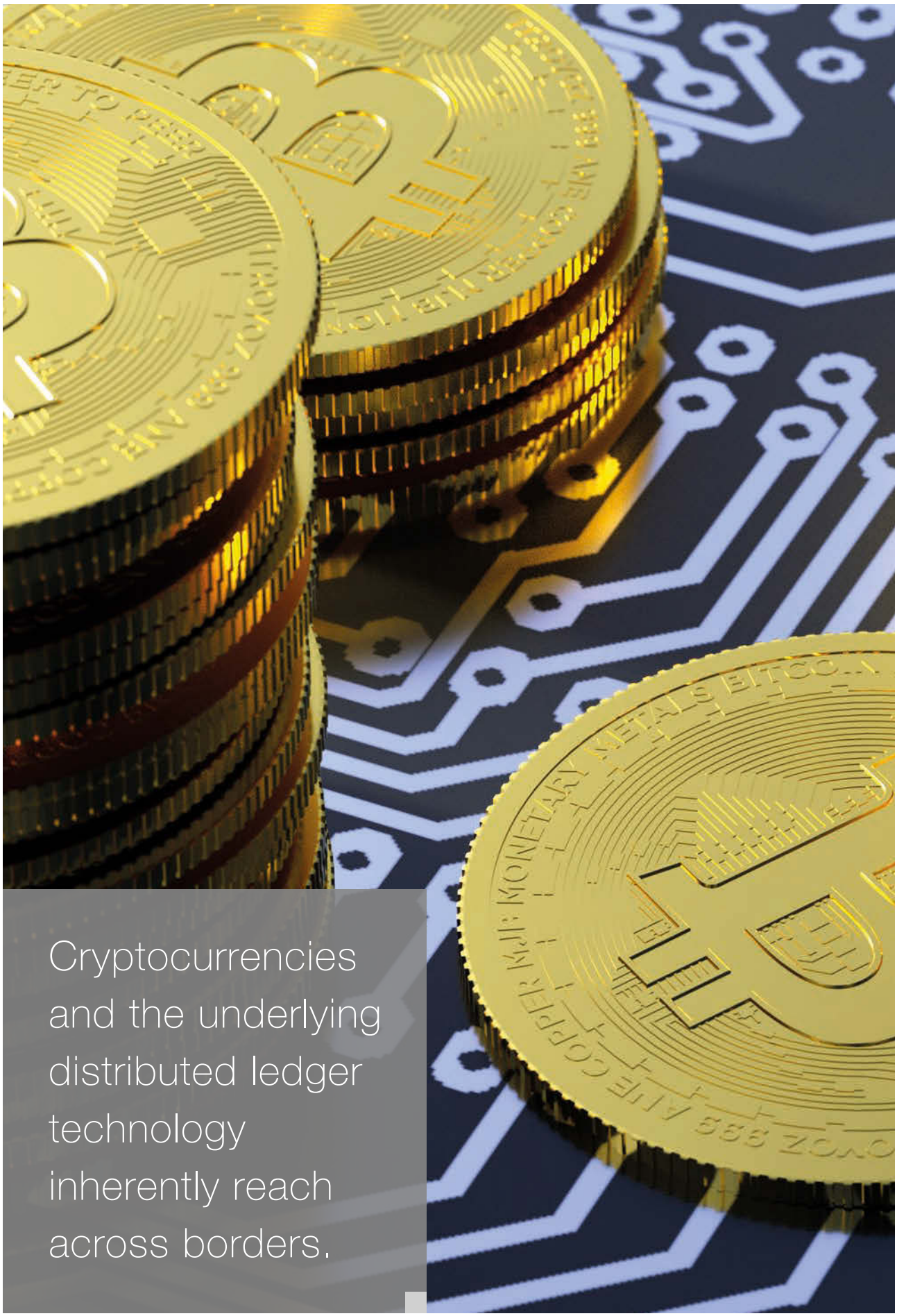
Health care data privacy and HIPAA compliance are central challenges to the implementation of blockchain technologies in the health care space, but have not slowed its innovation. There is significant potential for accurate, immutable records of health data between patients, insurers, and providers built on the blockchain. However, blockchain's pseudonymization methods pose a challenge as "the HIPAA Privacy Rule prohibits use of mathematically-derived pseudonyms because of potential re-identification of de-identified protected health information (PHI)," which, without additional innovation, "effectively makes blockchain non-HIPAA compliant."[350] While blockchain alone might not address these issues, the layering of additional privacy-focused technologies, such as Dynamic Data Obscurity or Intel's Software Guard Extensions technology (SGX), on top of a blockchain-based application, have begun to show promising results. PokitDok[351] has leveraged SGX-enabled Intel Chips to create "Dokchain," which "can perform what is known as 'autonomous auto-adjudication,'" such that once parties to a health care transaction have been verified, "the transaction between them can be processed instantly in a machine to machine communication based upon previously agreed upon smart contracts," significantly reducing the transaction costs of processing health care claims while remaining HIPAA-compliant by keeping all transacted data encrypted.[352] Another industry that highlights the paradox between transparency and privacy inherent in some potential uses for blockchain is banking and financial transactions. The ability to transact without having to rely on trust-based intermediaries to verify identity that blockchain offers could significantly alter everything from consumer banking to trading, but the transparency that blockchains could offer to businesses might also expose them to regulators and competitors in unwanted ways. Blockchains beyond Bitcoin have begun to offer a balance between transparency and privacy. Quorum, JPMorgan Chase's Ethereum-based blockchain, utilizes a dual-layered approach to the creation of blocks, whereby public data is verified initially and private details remain sequestered.[353] What separates this framework from Bitcoin's is a permission-based system that creates a hierarchy among participating nodes, such that only trusted parties interact on any given chain. Leveraging private blockchains and utilizing encryption are particularly applicable to privacy concerns with smart contract solutions.

Smart contracts

As elaborated on above in this whitepaper, smart contracts bring with them both potential theoretical solutions to privacy concerns with Bitcoin and blockchain-based applications, and additional complications that problematize privacy in practice. With respect to banking and financial transactions, smart contracts offer promising solutions to a number of privacy "pain points" along the timeline of any one transaction, but still face hurdles in maintaining privacy and security while meeting scalability requirements.

While encrypting data might assist with some privacy issues on a public blockchain like Bitcoin's, it would be difficult to scale to the level of transactional frequency any bank would require.[354] R3's Corda shared ledger platform seeks to address this challenge by "develop[ing] the blockchain in such a way that transactions that are published for verification purposes only contain a limited amount of data," essentially decreasing the amount of information that is exposed, and distributing data only to parties who need it. By utilizing Intel's SGX, Corda offers a "transaction verification layer" atop the blockchain that allows a transactional counterparty to "only obtain the result but not the inputs" of the transaction, which marries the structural benefits of blockchain with privacy protections offered by encrypted software that can run "without revealing…data to the owner of the hardware."[355] Encrypting instructions on the public/ private keys of a given blockchain in order to allow for automatic internal decryption and prevention of unauthorized viewing of sensitive input information will be particularly relevant in a future where trades might be recorded on blockchains, and competing banks want to avoid other market participants from free-riding or front-running on transactions that would otherwise appear fully transparent on the blockchain.[356]

Of course, every form of extensive activity is potentially subject to re-identification. This theoretically includes Bitcoin activity, in which re-identification is supposedly possible using information from the blockchain. Nevertheless, those using bitcoins and distributed ledger technology should be aware of the already-identified risks of re-identification inherent in the current model, and take steps to reduce such risks by incorporating encryption or obfuscation into their blockchains to protect seudonyms used, and linkable public information.



Cryptocurrencies and the underlying distributed ledger technology inherently reach across borders.

Intellectual Property

While Bitcoin made the blockchain famous, the benefits of a secure distributed ledger are being implemented across many fields. Ancillary technologies are being invented to improve and expand digital currency services, improve block mining, and utilize distributed ledger technologies in new ways. As with many technologies, the intellectual property rights surrounding blockchain technologies are quickly evolving and maturing—and becoming less open.

Satoshi Nakamoto published his idea for the blockchain underlying Bitcoin, placing the idea into the public domain for anyone to implement. But just because the original idea for the blockchain is in the public domain does not mean that projects based on that idea are, too. The Bitcoin project is distributed under the permissive MIT open source license that allows others to use, modify, and share the software.[357] Other digital currency and distributed ledger projects are similarly distributed under open source licenses, but the licenses vary. For example, Ethereum is under the GNU General Public License (GPL), but its core engine is under a more liberal license.[358] Litecoin is released under the MIT open source license.[359] And OpenChain is released under the Apache 2.0 license.[360] What does that really mean for companies using or interested in cryptocurrencies or other projects built on the blockchain? What are the specific terms of the open source licenses? Do patents cover blockchain technologies? And can new technologies built on the blockchain be patented? This chapter examines these questions and identifies emerging trends in blockchain IP. The IP landscape developing around blockchain technologies can be a minefield. Stakeholders and market entrants need to know how to navigate the risks and protect their contributions.

Bitcoin's open source license

The Bitcoin Project is released under the MIT License.[361] The MIT License grants any person with a copy of the licensed software the rights to copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the

software. Under the MIT License, however, copies and derivative works, such as substantial portions of the software, must include a copyright notice and terms.

Bitcoin has sparked development of third-party software, other cryptocurrencies, and other applications of blockchain technology. The Bitcoin Project encourages innovation, and the MIT License permits development of software and new technologies incorporating Bitcoin code. The license even allows for proprietary software to use Bitcoin software. Some Bitcoin-based software therefore may not be freely modified or copied. Companies utilizing Bitcoin software or other open source blockchain software therefore need to be aware of the terms of the license to the specific software they are using to understand their rights and potential liabilities.

Other blockchain application licenses

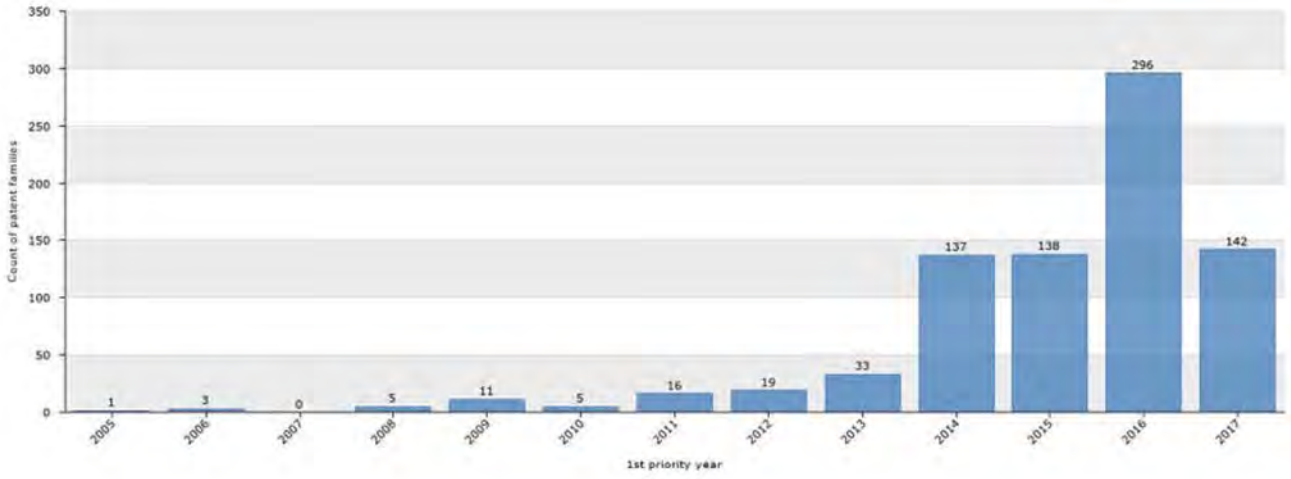
Many promising new technologies are developing based on the blockchain idea and its permissive license. The Hyperledger Project, for example, is a cross-industry, open source collaborative effort created to advance blockchain technology. Its stated mission is to create an enterprise grade, open source distributed ledger framework and code base, upon which users can build and run robust, industry-specific applications, platforms and hardware systems to support business transactions.[362] While the Hyperledger Project is open source, like the Bitcoin Project, its open source license is different from the MIT License under which the Bitcoin software is distributed. Inbound code contributions to the Hyperledger Project and outbound code will be made available under the Apache License, Version 2.0.[363] The Apache License V2.0 grants broad rights, but includes additional notice requirements and restrictions on derivative works not included in the MIT License. The Apache License V2.0 also grants a limited patent license from each contributor, but the limited license can terminate if a licensee institutes litigation relating to the open source project. Companies using or developing blockchain technologies that are unaware of the specific terms of relevant licenses risk infringement.

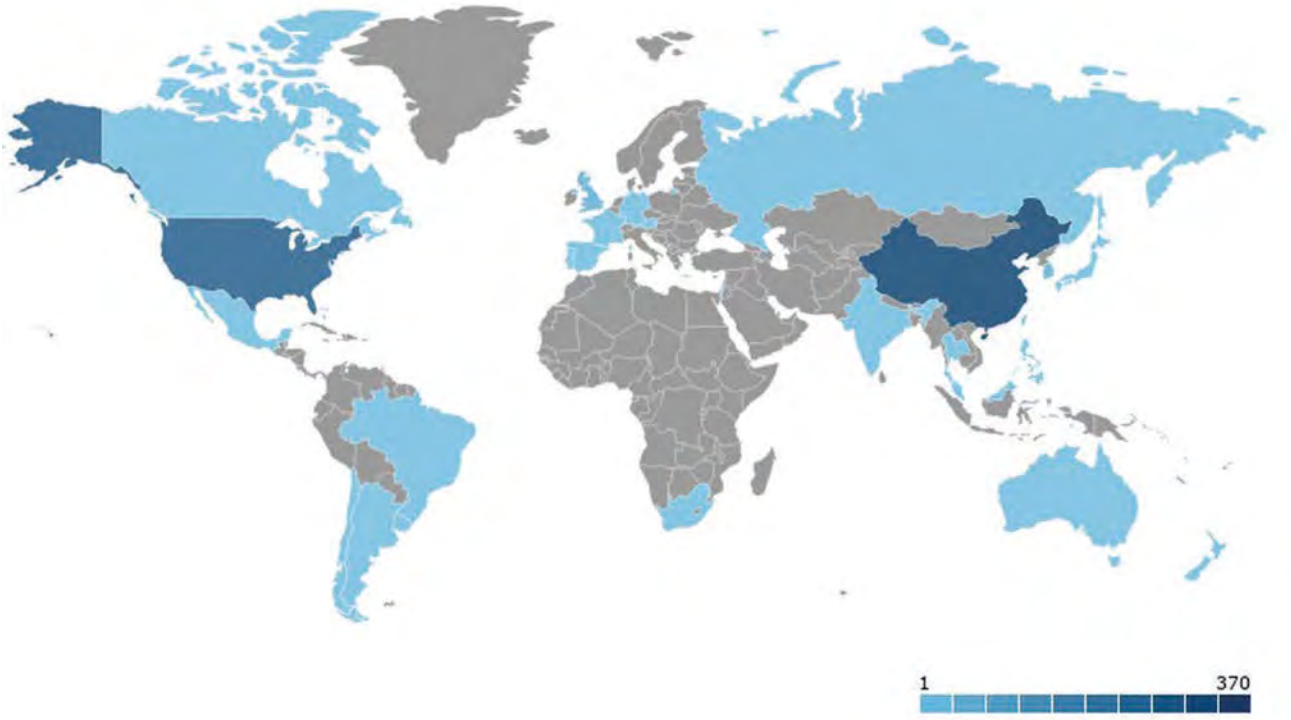
The rise of blockchain patents

The growth of Bitcoin has sparked innovations in supporting and complementary technologies. More innovation is expected as the applications of blockchain technology beyond cryptocurrencies continue to be explored. A sharp increase in patent applications in recent years evidences both the rate at which the technology is developing, and the desire of stakeholders to maintain their competitive advantage by protecting their inventions.

The below chart shows the number of new patent applications directed specifically to blockchain-related

Distribution of search results by 1st priority year

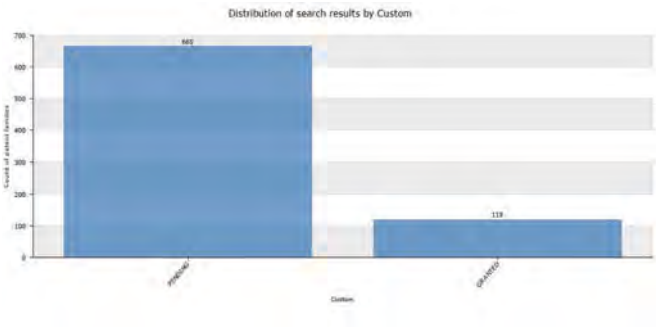




technologies filed per year from 2005 through 2016 on the horizontal axis.[364] As shown, there were almost nine times as many new patent filings in 2016 as there were in 2013. Patent applications can take 18 months to publish, so the data for 2016 remains incomplete. As more applications publish, we expect to find an even sharper rise.

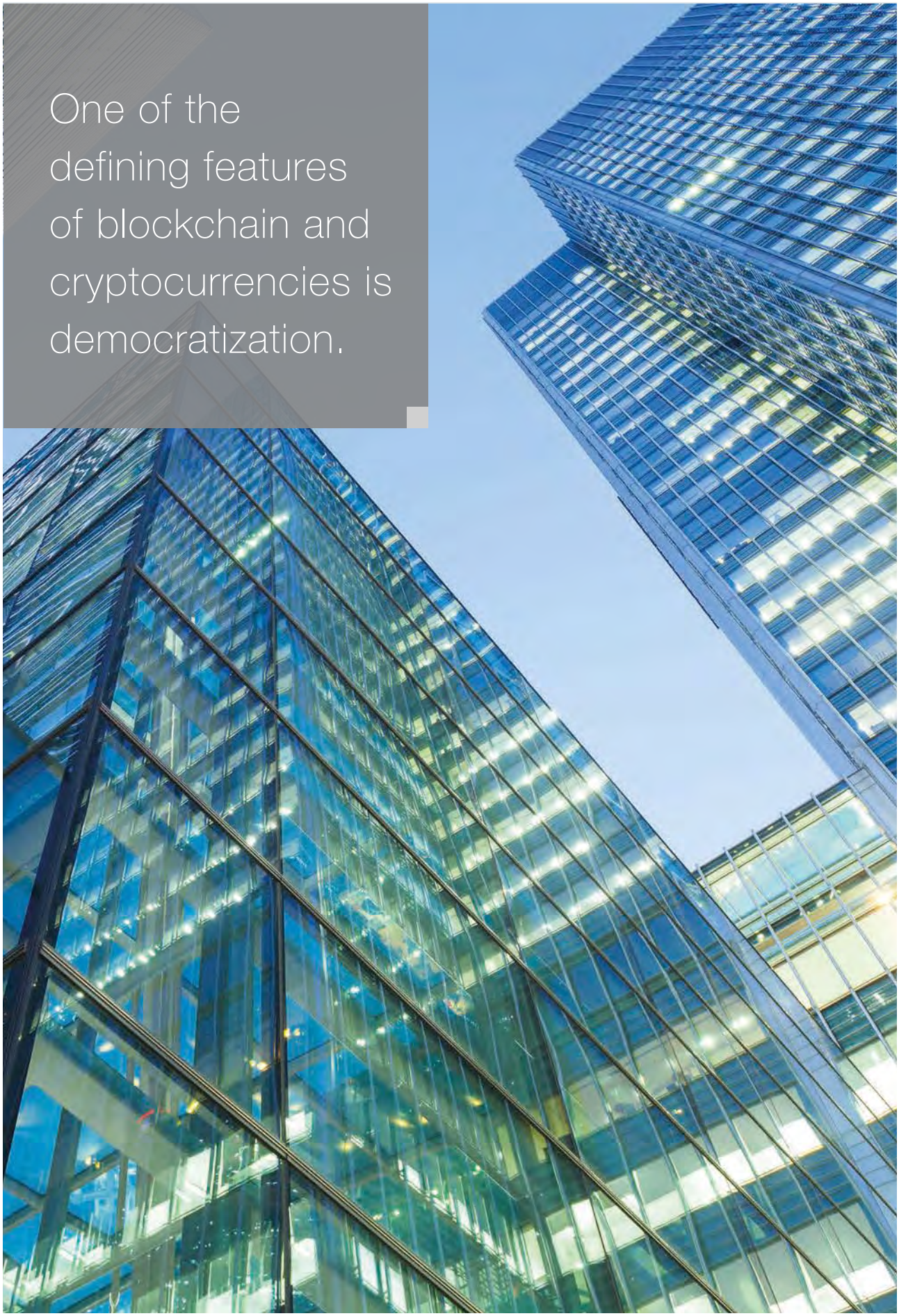
Cryptocurrencies and the underlying distributed ledger technology inherently reach across borders. Patent application filings provide an indication of anticipated markets for developing technology. The map below shows individual patent filings in each country, with darker blue indicating a greater number of filings.[365] While the greatest density of patent filings has been in North America and China, applications are being filed across Europe, Asia, South America, and Australia. An international patent minefield is developing, and market participants with an international reach need to know their international exposure. And because of the international reach of most blockchain-rooted technologies, innovators should consider international protection for their inventions.

Empirical analysis of global published applications shows that the largest numbers of patent applications cluster around payment methods and systems using cryptocurrencies or the block chain. Other areas of intense patent activity surround encryption technologies and blockchain mining technologies. As the technology implementing the underlying blockchain in other ways matures, we expect the areas of activity, and thus the areas of exposure to stakeholders, to expand.



The chart above shows that while 119 patents directed to blockchain-related technologies have issued, another 655 published applications are pending. Hundreds of other applications have not yet likely been published. Patent filings are on the rise and patent examination in most countries takes years, so the global landscape for issued patents relating to cryptocurrencies and other blockchain inventions is just now forming. It will be imperative for stakeholders and market entrants to protect their valuable IP, and understand the risks presented by the IP of others in this emerging IP landscae.

One of the defining features of blockchain and cryptocurrencies is democratization.



Social impact, responsibility and media

Despite being an emerging technology, Bitcoin has been the focus of several charity and social impact projects since its inception. While the use of bitcoins to fund charity projects and for remittances has garnered recent attention, there has been less focus on how the blockchain algorithm itself might be used in applications with a social impact. This chapter describes some successful applications of the blockchain algorithm to problems in the social responsibility, social media, and advertising spaces, and describes the many potential opportunities in this area.

Lowered transaction fees mean more money for causes

The immediate appeal of cryptocurrencies in the context of international aid is the potential to lower transaction and currency exchange fees, especially for smaller donation amounts. Donors can send small donations of fiat currency, which are converted to bitcoin, or another currency, at an approximately 1 percent transaction fee, which are in turn sent to an aid organization's digital wallet for conversion into a local currency of choice. By reducing these fees, organizations can make more out of smaller donations.

ChangeTip, a micropayment service, partnered with Direct Relief to enable donors to purchase $5 prenatal vitamin supplements for mothers in the developing world.[366] ChangeTip channeled these small donations through bitcoin, cutting down on fees that would have made such small donations impracticable. The accuracy and transparency offered by distributed ledger technology can also reduce reliance on external audit or intermediary functions for microfinance to poor and low income clients, for example, thus ensuring greater access to wealth and furthering the fight against poverty.[367]

Greater transparency

The Bitgive Foundation, partnering with Factom, previously launched the Donation Transparency Project,

which aims to track donations and expenditures in aid projects using the blockchain algorithm.[368] The platform aims to add transparency and traceability to international aid organizations, so that donors can see the impact of their giving and make informed decisions about effective aid organizations. Similar applications could improve the ability of governments and international charities alike to track international development spending, reduce corruption, and analyze trends across projects. Likewise, corporations can be held accountable by their customers or shareholders in a number of ways related to corporate responsibility, as discussed below.

Access to financial services

Applications of the blockchain algorithm have much to offer the more than 2 billion adults in the world who lack a bank account. Recent attention has focused on using cryptocurrencies to send remittances, which have typically been subject to high fees. However, while much has been said about the potential for Bitcoin to reduce fees for remittances,[369] building an end-to-end money transfer system using digital currency has remained difficult.

Currently, the most successful applications pick a single country or region and focus on the so-called "last mile," where the incoming money transfer is converted to cash for its recipient.[370] For example, BitPesa focuses on converting bitcoins to Kenyan or Tanzanian shillings and depositing that local currency to a mobile money number.[371] By relying on the pre-existing mobile money wallet system in use by many Kenyans and Tanzanians, BitPesa is able to sidestep the complicated international money transfer system that has made a general-purpose bitcoin-based remittance system so elusive. The Philippines, which is the world's third-largest recipient of remittances, has also seen significant innovation in using bitcoin to send money into the country. Several startups focus on converting bitcoins to Philippine pesos, and making cash available to remittance recipients in partnership with the ATM networks, convenience stores, and pawnshops that customers already use.

As with international aid, the blockchain algorithm has more to offer than simply reducing fees for money transfers. Coins.ph, one of the remittance startups in the Philippines highlighted above, has introduced a service called Teller.[372] Teller is like ridesharing for ATMs in that the Teller application connects customers to pre-screened tellers who can take or distribute cash in exchange for bitcoins. Tellers and customers are kept accountable through a two-way reviewing system, and its inaugural tellers are the same convenience stores and pawnshops that customers currently use for remittances. Because the financial transaction itself is secured by the blockchain, Teller can focus on the security and availability of only one step of the process: the exchange of an electronic balance for cash. Using the blockchain, in other words, makes it possible to serve the unbanked where they already are.

Financial empowerment

One of the defining features of blockchain and cryptocurrencies is democratization. For those who do not have control over their financial destinies under traditional financial systems, the blockchain opens up significant opportunities. For example, two projects started by Afghan entrepreneur Fereshteh Forough use bitcoin to pay Afghani women for work they complete as they learn skills for the digital economy. The Digital Citizens Fund[373] builds women-only computer centers to teach young women word processing, presentation, financial and Internet-based tasks, while Code to Inspire[374] similarly teaches young women computer programming. Both organizations use bitcoin to pay their students, not only because of the number of unbanked people in Afghanistan, but also because of the cultural, legal, and safety issues associated with giving women cash in that country.[375] With bitcoin, these young Afghani women can exercise a measure of control over their financial futures.

Blockchain-based services like WildSpark,[376] which compensates users for creating content, could further socio-economic independence through the opportunity

to create one's own marketplace, or even personalized or idea-based currencies linked to their businesses, before seeking funding, and, by extension, "participate in a miniature, virtualized, in-app economy."[377] The intersection of blockchain's potential impact and social investing is particularly evident in initial or independent coin offering.

Initial coin offerings (ICOs)

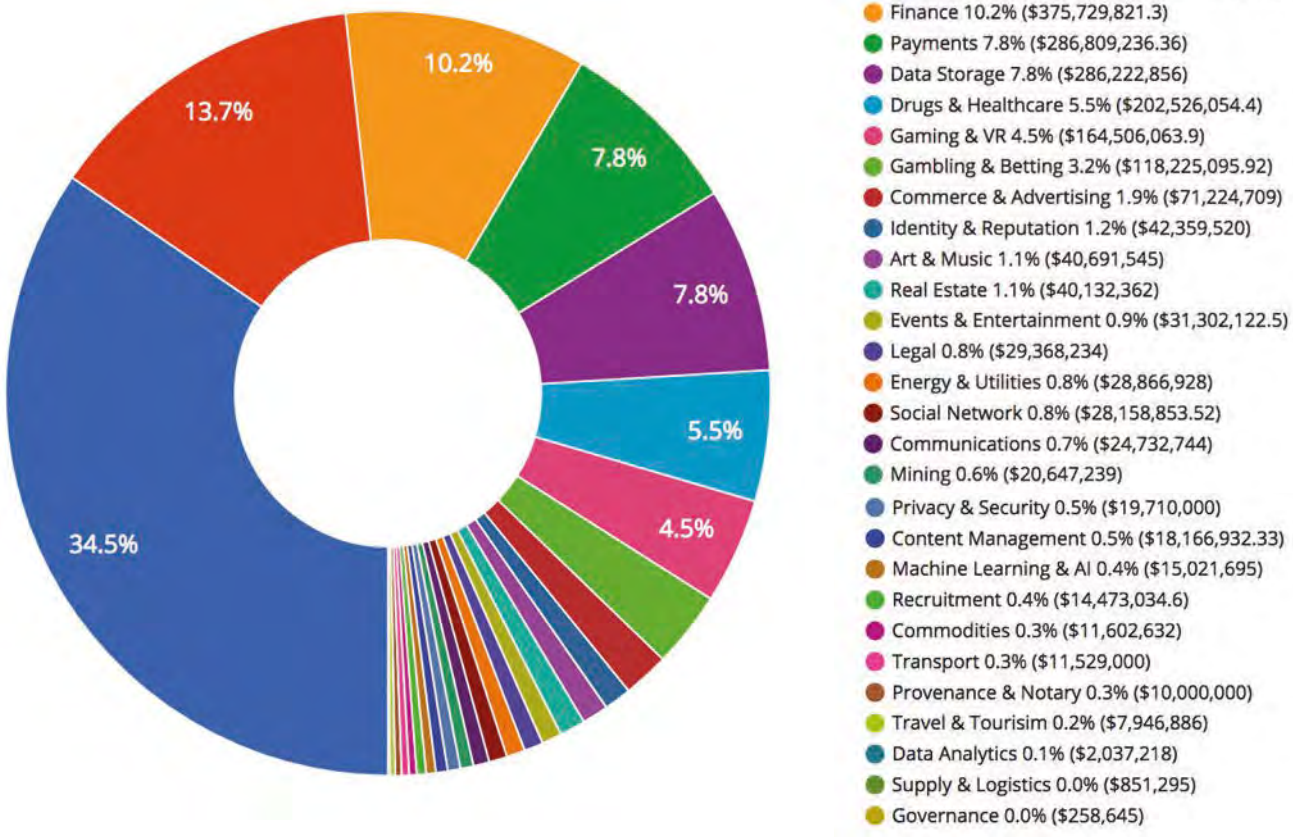
As we discussed in the "application in capital markets" chapter, blockchains and cryptocurrencies offer new and exciting ways for individuals to invest in new projects and initiatives. However, as with most new and innovative technologies, such investment will come with potential risks.

At its core, an ICO is a method of "crowdfunding" through the use of cryptocurrencies. In a mechanism similar to that like the more familiar IPO, a new digital asset (the "initial" coin being offered) is sold in exchange for legal tender or other pre-existing cryptocurrencies like bitcoin. ICOs could have far-reaching implications for start-up ventures, nonprofits and fundraising.

Various celebrities have publicized their support for ICOs. Such high-profile activity raises a number of issues that would require significant regulation from agencies such as the FTC and SEC. [378] An ICO touted by a celebrity might trigger additional or different responsibilities than those already in place for the more traditional celebrity endorsement of tangible merchandise.[379]

Like equity crowdfunding—a disruption that eventually led to the passage of the JOBS Act370 and other efforts to protect consumers engaging in social investment—ICOs have begun to garner attention from regulatory agencies such as the Consumer Financial Protection Bureau (CFPB).

ICOs by Category 2017



As detailed in the U.S. Regulatory section, in an August 2014 Advisory, the CFPB warned consumers of the potential risks associated with transacting with virtual currencies such as fraud or scams. 371 With the increasing prevalence and popularity of ICOs,[382] the CFPB may once again warn of the consumer protection risks associated with virtual currencies, especially because of the clouded nature of metrics such as market value associated with ICOs.[383] Similarly, certain ICOs could eventually face actions from the Federal Trade Commission (FTC) as they continue to be endorsed by social media influencers whose followers may seek them out as investment opportunities.[384] As such, the FTC may find it necessary to take action to prevent false advertising or other misleading behavor that could accompany some ICOs.[385]

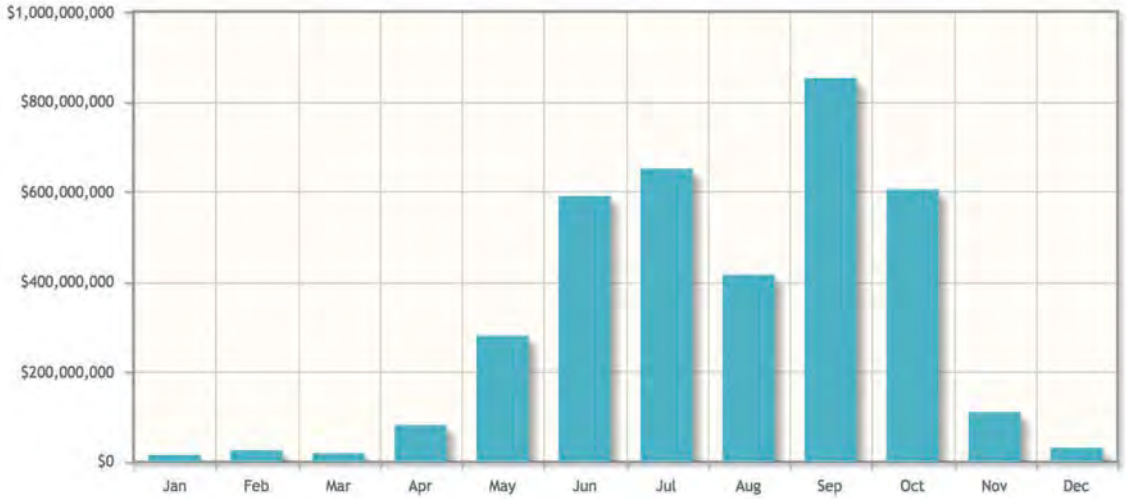
Blockchain, media and advertising

Digital advertising ICOs[386] and initiatives such as Comcast's "Blockchain Insights Platform" Blockchain seek to leverage blockchain technology to maximize ad targeting.[387] As part of such a strategy, permissioned parties may be able to use a blockchain to ensure that ads are securely delivered to the correct audience, thus reducing the risk of ad fraud while simultaneously decentralizing ad-delivery auditing. [388]

While the ubiquitous use of blockchain technology in advertising and marketing may still be a few years away, there is significant potential for the industry to use the technology in areas such as measuring ad interaction, and in ad exchanges. The concept proposed by BitTeaser is a good example of what early uses of this technology in the advertising sector may look like or what can be built upon. BitTeaser essentially sets up an ad exchange where users can pay for ads and accept ad revenues in a variety of digital currencies, including Bitcon.[389]

Companies in the fashion and food industries are also experimenting with new blockchain tools for verifying the authenticity of products in primary and secondary markets, building upon technologies such as RFID readers and tags. [390] For example, customers may be able to use mobile devices or other blockchain-specific devices that are able to scan tags or labels on merchandise to view information such as the designer or producer, the manufacturing location, or where the item was first modeled (e.g., apparel items in fashion shows). The same concept may be useful in other merchandise areas, such as with the diamond or fine art industries for verification purposes. [391] These technology-driven verification processes could encourage greater consumer confidence in purchases, while also reducing the risk of over-reliance on targeted advertising.

Cryptocurrency ICO Stats 2017



Social media

The effect of blockchain on social media is directly related to the privacy and security concerns surrounding existing social media platforms (and around the transparency of blockchain). Some companies are developing social media platforms using multi-tiered blockchains to keep transactions and messaging on the platform private. [392] Additionally, these new blockchain-based social media platforms are offering users the opportunity to engage in transactions using the digital asset offered by the platform. [393]

Improving governance and minimizing corruption

Blockchain may impact and modernize how information belonging to large groups of people or companies is stored and secured. [394] For example, a state government may be able to rely on blockchain to create a more open, transparent ledger of public information because of the technology's immutable qualities. The nation of Honduras already is experimenting with this concept to store land title records. [395] Honduras has historically faced the problem of an incomplete land title system that has fallen victim to corruption and manipulation.[396] The government of Honduras, working with a U.S.-based startup, is aiming to overhaul its current land record techniques to create an auditable, yet incorruptible, title database.[397]

Likewise, the U.S. title insurance industry could use blockchain to change how consumers buy and sell property. Currently, the Ethereum blockchain is being evaluated for such a purpose; however, it faces the challenges associated with monetizing and implementing a blockchain solution to an inefficient process such as title searching, especially without first convincing government entities to fully digitize public property records that are often in hard copy form. [398]

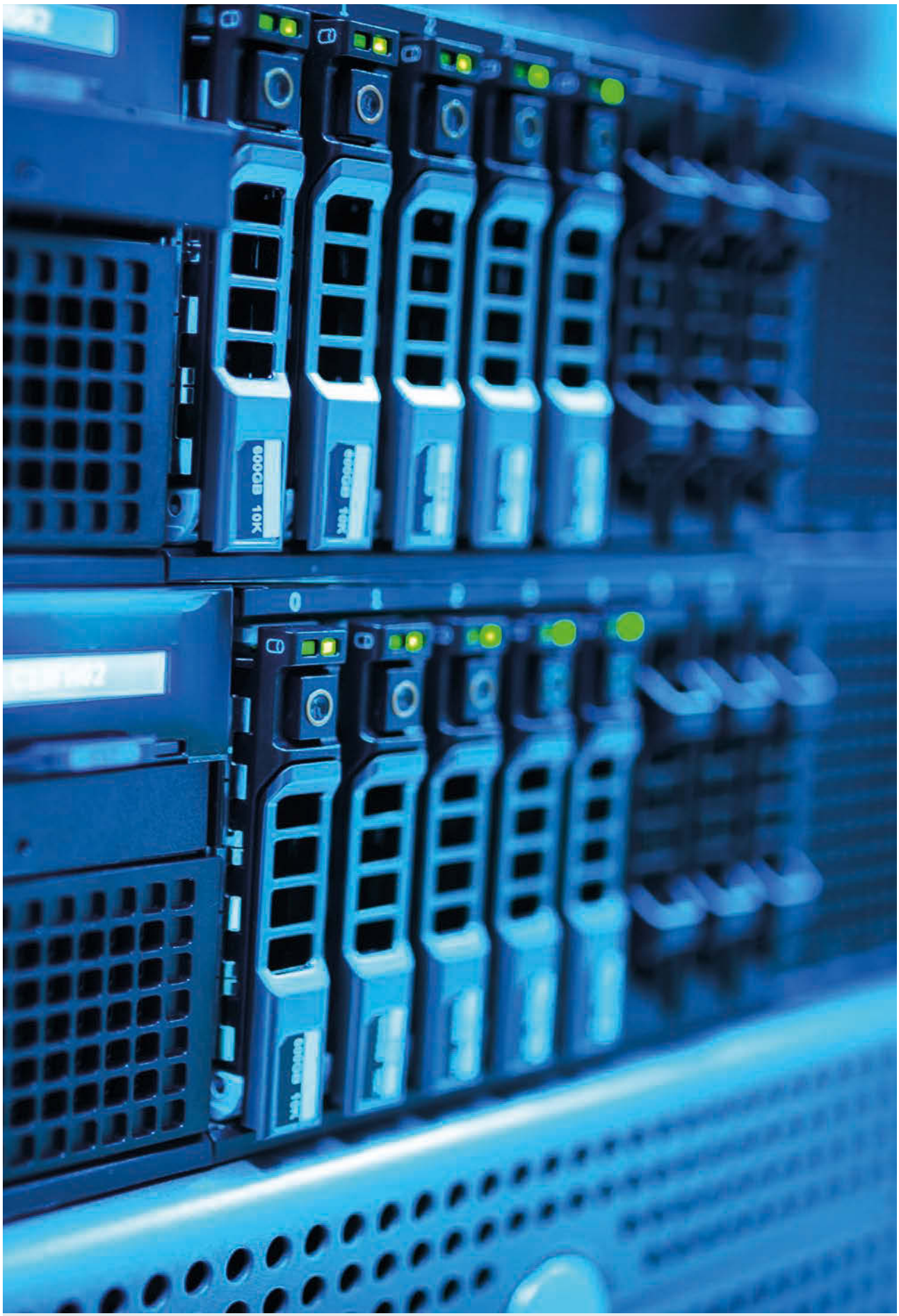
The state of Delaware's "Delaware Blockchain Initiative" is exploring ways to streamline corporate and governmental processes. Delaware will incorporate blockchain technology in the handling of official documents, such as title documents and birth certificates. The state also passed amendments to its laws to allow persons to issue and trade stocks on a blockchain. Initiatives such as this, if widely adopted, might bring increased transparency and efficiency to both government and private industry operations.

Corporate social responsibility

Companies can create public or semi-private blockchain networks where their customers are a part of the network. For example, some companies are considering whether loyalty point systems on a blockchain would be interesting to consumers. As part of a company network, customers could monitor and verify company activity to ensure that companies stay true to their promises, such as using only organic ingredients or sustainable materials. Because of the public nature of this potential type of blockchain, and the risk of consumer backlash if the company fails to keep a promise, companies may be encouraged to provide more transparency into their corporate practices. This in turn would encourage consumers to be more engaged in policing their favorite brands and holding them accountable for their promises.[399]

Summary

The initial successes and challenges of using cryptocurrencies for social impact projects have inspired a new wave of innovation focused on blockchain. We have only scratched the surface of the tremendous opportunity in this area, as entrepreneurs, nonprofits and institutions around the world look to find ways to use the blockchain algorithms to empower the developing world, reach those in need, reach a wider audience to encourage investment and innovation, and build a better future for all.


600GB 10K

Closing note

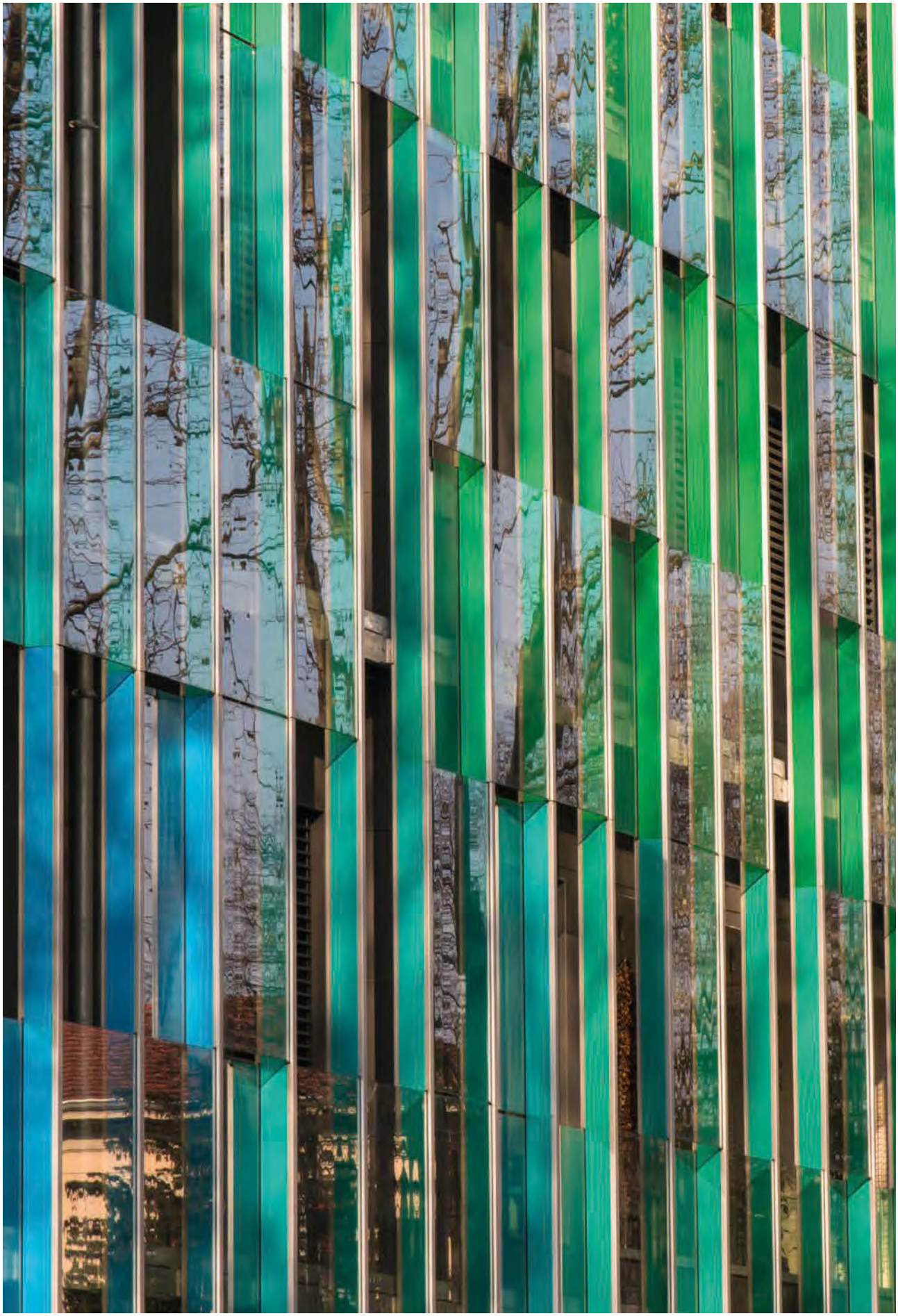
We trust that by now you have become comfortable with, and hopefully even enthusiastic about, the potential transformative power of blockchain technology. Many have compared the development of digital currencies and digital ledger technologies with the development and adoption of the Internet. At that time, many remained skeptical of the Internet's application to financial transactions, and to the financial world more generally. Today, we cannot imagine an economy and financial system without the capabilities that the Internet offers. In five to 10 years, we may be sharing the same view of blockchain technologies.

Of course, the development of online transactions and e-commerce has generated numerous unique regulatory and legal issues for financial institutions and other participants in the business and financial world. To the extent that blockchain will impact the financial system as much as some predict, the technology will similarly generate unique regulatory and legal issues that our clients must address. At Reed Smith, our focus on client services means staying ahead of the curve, and advising clients on the potential legal issues surrounding new technology as that technology develops. As your business or organization begins to devise strategies regarding digital currencies and blockchain technology, the Reed Smith Blockchain Technology Team and its members across our global offices are always available to advise you on the legal issues surrounding this exciting new technological development.

There is no doubt that DLT has the potential to effect significant changes in the financial world and other industries by providing the ability to have a transparent, generally immutable record of a transaction, without the need for trusted third parties. As has been discussed throughout this white paper, some of the most exciting potential applications of blockchain technology arise outside of the digital currency context. We hope that this white paper has provided you the tools to begin strategizing how blockchain may impact, or even transform, your business and operations.

Sincerely,

The Reed Smith Blockchain Technology Team



Glossary of terms

51% Attack (also Majority Attack)

The ability of someone controlling a majority of network hash rate or mining power to revise transaction history and prevent new transactions from confirming.

Bit

Bit is a common unit used to designate a sub-unit of a bitcoin – 1 million bits is equal to 1 bitcoin (BTC or ฿). This unit is usually more convenient for pricing tips, goods and services.

Bitcoin

Bitcoin - with capitalization, is used when describing the concept of Bitcoin, the Bitcoin protocol, or the entire network itself, e.g., “I was learning about the Bitcoin protocol today.”

bitcoin - without capitalization, is used to describe bitcoins as a unit of account, e.g., “I sent 10 bitcoins today.” It is also often abbreviated BTC or XBT.

Bitcoin exchange

A marketplace that allows people to buy or sell bitcoins using different currencies. Because of the blockchain algorithm, exchanges can be made securely upon transfer.

BitLicense

A popular name for the business license (and its associated regulations) issued by the New York Department of Financial Services (NYDFS) under regulations that came into effect August 8, 2015, designed for companies engaged in virtual currency business activities.

Block

A unit of data containing information regarding transactions that have occurred during a period of time. A block contains the hash code of the previous block in the blockchain, a set of transactions that are recorded in that block, and (if it exists), a reference to the following block in the blockchain.

Blockchain

A blockchain is a public ledger of all bitcoin transactions that have ever been executed. The term may also be used to more generally describe the distributed ledger technology utilized by the Bitcoin blockchain, even if applied outside of the Bitcoin context.

Block height

A measure of the age of a digital ledger—the more blocks that are solved and added to the ledger, the higher the block height. When choosing between two distributed ledgers, the one with the higher block height will often be more secure, and therefore more likely to be accurate.

Byzantine generals problem

An abstraction of a computer system problem concerning the handling of malfunctioning components

that give conflicting information to different parts of the system:

> A group of generals of the Byzantine army is camped with their troops around an enemy city, and communicate only by messengers. The generals must agree upon a common battle plan; however, one or more of the generals may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors.

Bitcoin has frequently been extolled for solving the Byzantine Generals Problem with its applications of proof of work and consensus.

Cold storage

The storage of a reserve of bitcoins or private keys offline, i.e., disconnected from the Internet, in a physical storage device such as a hard drive or USB storage device.

Consensus

A requirement for updating certain distributed ledgers requiring a sufficient number of participants to agree (usually more than half) before accepting the update as accurate.

Distributed consensus

Refers to consensus from the various different computers making up the network coming to an agreement without the need for a central control unit making that determination, and then broadcasting it to the rest of the network This is at the crux of how Bitcoin operates.

Federated consensus

Consensus achieved under what is known as a federated Byzantine agreement system, whereby consensus can be achieved from a "quorum slice," a subset of trustworthy nodes that have earned trust organically on the system over time.

Crypto asset

Tokens that are digital representations of value or utility within an ecosystem. For example, CME's Royal Mint Gold (RMG) token is a digital representation of physical gold stored in a Royal Mint vault. Digital assets include virtual currency, tokenized securities, tokenized commodities, cryptocurrencies, etc.

Cryptocurrency

A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

Cryptography

The use of mathematics to secure information and to convert data into a secret code for transmission over a public network. Today, most cryptography is digital, and the original text ("plaintext") is turned into a coded equivalent called "ciphertext" via an encryption algorithm.

Cryptographic hash function

A hash function that takes an input (or "message") and returns a fixed-size alphanumeric string, which is called the hash value (sometimes called a message digest, a digital fingerprint, a digest, or a checksum).

The ideal hash function has three main properties:

- It is extremely easy to calculate a hash for any given data.
- It is extremely computationally difficult to calculate an alphanumeric text that has a given hash.
- It is extremely unlikely that two slightly different messages will have the same hash.

Cypherpunk

An activist advocating widespread use of strong cryptography as a route to social and political change. Cypherpunks have been engaged in an active movement since the late 1980s.

Digital currency (also e-currency, e-money, electronic cash, electronic currency, digital cash, cyber currency, virtual currency)

An electronic medium of exchange in which a person can securely pay for goods or services electronically without necessarily involving a bank to mediate the transaction.

Digital signature

The combination of a public key, which identifies you to others, and a private key, which allows you to access secret information. Blockchain uses public keys to identify participants in the ledger, and requires private keys to allow participants to access assets recorded on the ledger.

Distributed consensus

See *Consensus*

Distributed Ledger Technology or DLT

A record of transactions that is shared over a network with others without a central server or entity that others must connect to, and the technology that provides such digital ledger.

Double spending

Double spending is the result of successfully spending the same unit of currency (e.g., the same bitcoin) more than once. Bitcoin protects against double spending by verifying each transaction added to the blockchain to ensure that the inputs for the transaction had not previously been spent.

Federated consensus

See *Consensus*

Fork

When miners produce simultaneous blocks at the end of the blockchain, each node individually chooses which block to accept. Absent other conditions that suggest a more stable block, nodes usually use the first block they see, and the problem is resolved once one chain has more proof of work than the other.

Hard fork

A permanent divergence in the blockchain. A hard fork may occur when upgraded nodes follow newer consensus rules previously considered invalid, and therefore newer nodes would recognize blocks as valid that older nodes would reject. This will cause non-upgraded nodes to not recognize and validate blocks created by upgraded nodes that follow newer consensus rules, creating a divergence.

Soft fork

A temporary fork in the blockchain. A soft fork may occur when miners using non-upgraded nodes violate a new, stricter consensus rule of updated nodes. This would lead to non-upgraded nodes accepting certain blocks, while updated nodes would reject these same blocks. Provided that a majority of nodes become updated, a permanent fork in the blockchain may be avoided.

Hash

A kind of algorithm that converts a string of data (of any size) into another, usually smaller, fixed-size output in a reasonable amount of time. Generally, hashes are "one-way," which means that if you have the hash, you don't know the original value. Hashes are used in cryptography to compare and verify data without having to see the original.

Hot storage

Refers to keeping a reserve of bitcoins on a web-based storage device or wallet.

Initial coin offering (or ICO)

Refers to a fundraising mechanism in which entities sell new digital tokens in exchange for cash, bitcoin or ether. Often the token provides the purchaser with an intangible right to a good or service, like a digital coupon. These tokens are often referred to as a "utility" token. An ICO is somewhat similar to an Initial Public Offering ("IPO") in which investors purchase shares of a company, and the ICO tokens may deemed securities if they meet the relevant regulatory definition.

Merkle tree (or hash tree)

A cryptography term that refers to a data structure made up of linked nodes, called a tree. A Merkle tree is a tree in which every non-leaf node (a node with children) is labeled with the hash of the labels of its children nodes. Hash trees are useful because they allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.

Mining / miner

Mining is the process of making computer hardware do mathematical calculations to solve new blocks to add to the blockchain. In the case of Bitcoin, miners are rewarded with newly minted bitcoins. But in other applications of blockchain, miners may be rewarded in a different way, or not at all.

Mining pool

Groups of people who mine together as a single unit in order to successfully mine faster by pooling computing resources.

Multi-signature address

A multi-signature address is associated with more than one private key.

Node

A node is a point of intersection/connection within a network. Any computer that connects to the Bitcoin network is called a node. Nodes share a copy of the blockchain and relay transactions to other nodes.

Nonce

The name for the string of digits that is added to a new block by miners when attempting to add this new block to the blockchain. The goal is to find the nonce that, when linked with the previous hash and the list of transactions comprising the new block, will produce a hash output falling below a certain target value. Once the correct nonce is found, the new block is added to the blockchain. Because it is impossible to predict which nonce will result in the correct target value, such a calculation involves computing and re-computing a hash output for numerous nonce values by "brute force." Presentation of the new block with the correct nonce value constitutes proof of work.

Peer-to-peer

Describes a type of network where each participant is considered equal. Peer-to-peer networks share information without a central server, controller, or authority. Participants are often connected to a few neighbors that will pass information to the rest of the network, and vice versa.

Proof of stake

Proof of stake is a method by which a cryptocurrency blockchain network aims to achieve distributed consensus. While the proof-of-work method asks users to repeatedly run hashing algorithms to validate electronic transactions, proof of stake asks users to prove ownership of a certain amount of currency (their "stake" in the currency). Peercoin was the first cryptocurrency to launch using proof of stake.

Proof of work

Data that is difficult to produce, but easy to verify. Blockchain uses proof of work to ensure new blocks of records added to the ledger are legitimate, because the miner invested work in producing the new block.

Private key

The unpublished key in a public key cryptographic system, which uses a two-part key: one private and one public. The private key is kept secret and never transmitted over a network. Contrast with "public key," which can be published on a website or sent in an ordinary email message.

Public key

An encryption key that can be made public or sent by ordinary means, such as by an email message. See also private key and public key cryptography.

Public key cryptography

A cryptographic system in which a two-part key is used: one public key and one private key.

Satoshi

The smallest usable denominations of bitcoin value. One bitcoin equals 100 million satoshis.

Satoshi Nakamoto

The pseudonym of a person or group of people who created the Bitcoin protocol and reference software, Bitcoin Core (formerly known as Bitcoin-Qt).

Silk Road

Silk Road was an online black market and the first modern darknet (a network overlay that is only accessible by using non-standard communications protocols and ports) market, best known as a platform for selling illegal drugs. All products sold on the site could be purchased anonymously with bitcoin.

Smart contract

Contracts allowing for contract performance to be verified and technically enforced, without requiring a judicial system or other centralized third party. While implementation of these new solutions is still fairly theoretical, a number of companies are actively building software solutions for smart contracts.

Sybil attack

An attack to the Bitcoin network where an attacker attempts to fill the network with nodes disguised to appear as unique network participants, but which in reality are nodes controlled by the attacker.

Virtual currency

"Virtual currency" is a legal or regulatory term of art. The term is defined by the European Central Bank as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community," and by the European Banking Authority as "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically." The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Treasury Department, has also defined virtual currency in its guidance published in 2013. It is often the term used in regulatory regimes to refer to all digital currency, including bitcoin, but in practice is often used only to refer to a currency not usable outside of its electronic platform, e.g., World of Warcraft "Gold".[400]

Wallet

The digital equivalent of a physical wallet containing private key(s). Each wallet can show the total balance of all bitcoins it controls, and lets users pay a specific amount to a specific person.

Key contacts

FinTech Leadership

Kari S. Larsen
Counsel
New York
+1 212 549 4258
klarsen@reedsmith.com

Herbert F. Kozlov
Partner
New York
+1 212 549 0241
hkozlov@reedsmith.com

Global Corporate Group

Gerard S. Difiore
Partner
New York
+1 212 549 0396
gdifiore@reedsmith.com

Aron S. Izower
Partner
New York
+1 212 549 0393
aizower@reedsmith.com

Katherine Yang
Counsel
Beijing
+86 10 6535 9532
kyang@reedsmith.com

Sai Pidatala
Partner
Dubai
+971 (0)4 709 6317
spidatala@reedsmith.com

Financial Industry Group

Claude Brown
Partner
London
+44 (0)20 3116 3662
cbrown@reedsmith.com

Tim Dolan
Partner
London
+44 (0)20 3116 3022
tdolan@reedsmith.com

Simon Grieser
Partner
Frankfurt
+49 (0)69 22228 9823
sgrieser@reedsmith.com

Ashley L. Shively
Counsel
San Francisco
+1 415 659 5695
ashively@reedsmith.com

Karen Butler
Associate
London
+44 (0)20 3116 3058
kbutler@reedsmith.com

Olga Newman
Associate
London
+44 (0)20 3116 3823
onewman@reedsmith.com

Evan R. Thorn
Associate
Washington D.C.
+1 202 414 9204
ethorn@reedsmith.com

IP, Tech & Data

Clark W. Lackert
Partner
New York
+1 212 549 0453
clackert@reedsmith.com

Mark S. Melodia
Partner
New York
+1 212 205 6078
mmelodia@reedsmith.com

Cynthia O'Donoghue
Partner
London
+44 (0)20 3116 3494
codonoghue@reedsmith.com

Gerard M. Stegmaier
Partner
New York
+1 202 414 9293
gstegmaier@reedsmith.com

Gerard M. Donovan
Counsel
Washington D.C.
+1 202 414 9224
gdonovan@reedsmith.com

Njeri S. Chasseau
Associate
New York
+1 212 549 4184
nchasseua@reedsmith.com

Sonny S. Grewal
Associate
Washington D.C.
+1 202 414 9272
sgrewal@reedsmith.com

Energy & Natural Resources

Brett Hillis
Partner
London
+44 (0)20 3116 2992
bhillis@reedsmith.com

Peter O. Zaman
Partner
Singapore
+65 6320 5307
pzaman@reedsmith.com

Simone Goligorsky
Associate
London
+44 (0)20 3116 3791
sgoligorsky@reedsmith.com

Alex G. Murawa
Associate
London
+44 (0)20 3116 3553
amurawa@reedsmith.com

Michael S. Selig
Associate
Washington D.C.
+1 202 414 9287
mselig@reedsmith.com

Insurance Recovery

J. Andrew Moss
Partner
Chicago
+1 312 207 3869
amoss@reedsmith.com

Carolyn H. Rosenberg
Partner
Chicago
+1 312 207 6472
crosenberg@reedsmith.com

Shipping

Noah T. Jaffe
Associate
New York
+1 212 549 0263
njaffe@reedsmith.com

Rebecca Lewis
Associate
London
+44 (0)20 3116 3847
rlewis@reedsmith.com

Endnotes

The mysterious origins of blockchain

1 http://fortune.com/2017/08/22/bitcoin-ethereum-blockchain-cryptocurrency/
2 https://www.coindesk.com/delaware-house-passes-historic-blockchain-regulation/
3 https://www.coindesk.com/arizona-smart-contract-clarity-winning-startups/
4 https://www.coindesk.com/barclays-stole-blockchain-spotlight-2016/; https://www.reuters.com/article/us-dtcc-blockchain-repos/dtcc-completes-blockchain-repo-test-idUSKBN1661L9; https://www.cryptocoinsnews.com/asx-increasingly-confident-blockchain-replacing-chess/
5 http://radar.oreilly.com/2015/01/understanding-the-blockchain.html
6 https://bitcoin.org/bitcoin.pdf

Blockchain 101

7 The terms "cryptocurrency," "virtual currency," and "digital currency" are sometimes incorrectly used interchangeably. "Digital currency" is the broadest term, and means an Internet-based medium of exchange with characteristics similar to physical currencies. "Virtual currency" is a subset of digital currency, and is defined by the European Banking Authority as "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically." Finally, "cryptocurrency" is a subset of "virtual currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds.
8 "Bitcoin" with a capital B refers to the protocol or software, whereas "bitcoin" (lower case b) refers to the unit of currency.
9 "Encryption at rest" refers to the practice of storing data in an encrypted form so that only the owner of a digital key or password can access it.
10 https://www.cnbc.com/2017/05/26/canada-backs-off-blockchain-interbank-payment-system.html
11 https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf

Smart contracts

12 https://www.cnbc.com/2016/04/19/barclays-used-blockchain-tech-to-trade-derivatives.html
13 http://www.dtcc.com/news/2016/april/07/successful-blockchain-test-completed

U.S. regulatory landscape

14 The term "virtual currency" is used by various U.S. agencies as a legal term that is defined to incorporate digital currencies and, in some cases, other types of crypto assets.
15 Sydney Ember, New York Proposes First State Regulations for Bitcoin, New York Times DealBook (July 17, 2014), http://dealbook.nytimes.com/2014/07/17/lawsky-proposes-first-state-regulations-for-bitcoin/?_r=0.
16 23 N.Y.C.R.R. Part 200 (Virtual Currencies), available at http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf (hereinafter, "BitLicense").
17 New York Department of Financial Services Press Release: DFS Grants Virtual Currency License to XRP II, LLC, an Affiliate of Ripple (June 13, 2016), http://www.dfs.ny.gov/about/press/pr1606131.htm. .
18 New York Department of Financial Services Press Release: DFS Authorizes Coinbase, Inc. to Provide Additional Virtual Currency Products and Services (Mar. 22, 2017), http://www.dfs.ny.gov/about/press/pr1703221.htm.
19 Id.
20 New York Department of Financial Services, Press Release: NYDFS Announces Approval of First BitLicense Application from a Virtual Currency Firm (Sept. 22, 2015), http://www.dfs.ny.gov/about/press/pr1509221.htm https://www.circle.com/en/investors.
21 New York Department of Financial Services Press Release: DFS Grants Virtual Currency License to XRP II, LLC, an Affiliate of Ripple (June 13, 2016), http://www.dfs.ny.gov/about/press/pr1606131.htm.
22 New York Department of Financial Services Press Release: DFS Authorizes Coinbase, Inc. to Provide Additional Virtual

Currency Products and Services (Mar. 22, 2017), http://www.dfs.ny.gov/about/press/pr1703221.htm
23 Id.
24 See, e.g., Daniel Roberts, Bitcoin company ditches New York, blaming new regulations, Fortune (June 11, 2015), http://fortune.com/2015/06/11/bitcoin-shapeshift-new-york-bitlicense/.
25 BitLicense § 200.2(p).
26 Id. § 200.3(a).
27 Id. § 200.2(q).
28 Nermin Hajdarbegovic, Lawsky: Bitcoin Developers and Miners Exempt from BitLicense, CoinDesk (Oct. 15, 2014), http://www.coindesk.com/lawsky-bitcoin-developers-miners-exempt-bitlicense/.
29 Id
30 BitLicense § 200.2(q).
31 Id. § 200.2(q)(1).
32 Id. §§ 200.3(a), 200.4, 200.5, 200.21.
33 Id. § 200.6.
34 Id.
35 Id. § 200.4(c).
36 Id. § 200.10.
37 Id. § 200.6.
38 Id. §§ 200.12(a), 200.15.
39 Id.
40 Id.
41 Id.
42 Id.
43 Id.
44 Id.
45 Id. § 200.8.
46 Id. § 200.9.
47 Id. § 200.12.
48 Id. § 200.19.
49 Id. § 200.20.
50 Id. § 200.18.
51 Id. § 200.19(g).
52 Id. § 200.16.
53 Id. § 200.17.
54 Id. § 200.13.
55 Id. § 200.14.
56 Conn. Gen. Stat. § 36a-596(14).
57 Conn. Gen. Stat. §§ 36a-598(11); 600(c), (d), 602(a).
58 N.H. Rev. Stat. Ann. §§ 399-G:1(XVI)(b); 399-G:2.
59 N.H. Rev. Stat. Ann. §§ 399-G:1(VII), (XV).
60 New Hampshire House Bill 436 (2017), https://legiscan.com/NH/text/HB436/id/1456175.
61 Coindesk, New Hampshire Governor Signs Bitcoin MSB Exemption Into Law, June 7, 2017, available at http://www.coindesk.com/new-hampshire-governor-signs-bitcoin-msb-exemption-law/.
62 N.C. Gen. Stat. § 53-208.42(20).
63 N.C. Gen. Stat. § 53-208.42(13)(b).
64 North Carolina Commissioner of Banks, Money Transmitter Frequently Asked Questions, http://www.nccob.gov/Public/financialinstitutions/mt/mtfaq.aspx (last visited Apr. 20, 2017).
65 Pete Rizzo, North Carolina Governor Signs Bitcoin Bill into Law, CoinDesk (July 6, 2016), http://www.coindesk.com/north-carolina-governor-signs-bitcoin-bill-law/.
66 Coindesk, Virtual Currency in Washington State: What Changes in July, June 8, 2017, available at http://www.coindesk.com/virtual-currency-changes-washington-state-money-transmitter-law/.
67 Washington State Department of Financial Institutions, Bitcoin and Virtual Currency Regulation, http://www.dfi.wa.gov/bitcoin.
68 Kansas Office of the State Bank Commissioner, Regulatory Treatment of Virtual Currencies under the Kansas Money Transmitter Act, Guidance Document MT 2014-01 (June 6, 2014), available at http://www.osbckansas.org/mt/guidance/mt2014_01_virtual_currency.pdf; Texas Department of Banking, Regulatory Treatment of Virtual Currencies under the Texas Money Services Act, Supervisory Memorandum – 1037 (April 3, 2014), available at http://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf; Tennessee Department of Financial Institutions, Memorandum: Regulatory Treatment of Virtual Currencies under the Tennessee Money Transmitter Act (Dec. 16, 2015), available at http://www.tennessee.gov/assets/entities/tdfi/attachments/2015-12-16_TDFI_Memo_on_Virtual_Currency.pdf; Illinois Department of Financial and Professional Regulation (IDFPR): Request for Comment, Digital Currency Regulatory Guidance (Nov. 30, 2016), available at https://www.idfpr.com/news/PDFs/IDFPRRequestforCommentsDigitalCurrencyRegulatoryGuidance2016.pdf..
69 Illinois Department of Financial and Professional Regulation (IDFPR): Request for Comment, Digital Currency Regulatory Guidance (Nov. 30, 2016), available at https://www.idfpr.com/news/PDFs/IDFPRRequestforCommentsDigitalCurrencyRegulatoryGuidance2016.pdf.
70 Coinbase, Coinbase accounts – Hawaii (Feb. 27, 2017), https://support.coinbase.com/customer/portal/articles/2754027.
71 Id.; Haw. Rev. Stat. § 489D-8.
72 N.C. Gen. Stat. § 53-208.42(17)(i).
73 Coinbase, Coinbase accounts – Hawaii (Feb. 27, 2017), https://support.coinbase.com/customer/portal/articles/2754027.
74 Id.
75 State of Wisconsin Department of Financial Institutions, Sellers of Checks, https://www.wdfi.org/fi/lfs/soc/ (last accessed April 19, 2017).
76 Id.
77 Florida v. Espinoza, Case No. F14-2923, Order Granting Defendant's Motion to Dismiss the Information (Fla. 11th Cir. Ct. July 22, 2016), available at http://www.miamiherald.com/latest-news/article91701087.ece/BINARY/Read%20the%20ruling%20(.PDF).
78 Id.
79 Conference on State Bank Supervisors, State Regulatory Requirements for Virtual Currency Activities, CSBS Model Regulatory Framework (Sept. 15, 2015), available at https://www.csbs.org/regulatory/ep/Documents/CSBS-Model-Regulatory-Framework%28September%2015%202015%29.pdf.
80 Id.
81 A.B. 1326, Cal. Leg. 2015-2016 Reg. Sess. (Cal. 2015), available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1326.
82 Id.
83 Yessi Bello Perez, California's Bitcoin Bill Shelved by State Senator, CoinDesk (Sept. 16, 2015), http://www.coindesk.com/californias-bitcoin-bill-shelved-by-state-senator/; Brian Doherty, California Bitcoin Regulatory Bill Pulled by its Sponsor, reason.com (Aug. 22, 2016), http://reason.com/blog/2016/08/22/california-bitcoin-regulatory-bill-pulle.
84 Merkle Tree, US State-level Digital Currency Law & Regula-

tion, http://merkletree.io/blog/2015/07/us-state-level-digital-currency-law-regulation/.

85 ReedSmith Client Alert, New State Blockchain Legislation, June 19, 2017, available at https://www.reedsmith.com/en/perspectives/2017/06/new-state-blockchain-legislation.

86 Id.

87 Coindesk, Arizona's Blockchain Gun Tracking Bill is Close to Becoming Law, Apr. 19, 2017, available at http://www.coindesk.com/arizonas-blockchain-gun-tracking-bill-close-becoming-law/; Buckley Sandler, Vermont Governor Enacts Law Including Blockchain Application, available at https://buckleysandler.com/blog/2017-06-14/vermont-governor-enacts-law-including-blockchain-application.

88 Vermont General Assembly, S.135 (Act 69), available at http://legislature.vermont.gov/bill/status/2018/S.135.

89 Hawaii House Bill 1481, available at https://legiscan.com/HI/bill/HB1481/2017.

90 Stan Higgins, Illinois Lawmakers Pass Bill Forming Blockchain Task Force, Coindesk (June 30, 2017), available at https://www.coindesk.com/illinois-lawmakers-pass-bill-forming-blockchain-task-force/.

91 Illinois Partners with Evernym to Launch Birth Registration Pilot, The Illinois Blockchain Initiative (Aug. 31, 2017), available at https://illinoisblockchain.tech/illinois-partners-with-evernym-to-launch-birth-registration-pilot-f2668664f67c; John Mirkovic, Blockchain Cook County — Distributed Ledgers for Land Records, The Illinois Blockchain Initiative (May 31, 2017), available at https://illinoisblockchain.tech/blockchain-cook-county-final-report-1f56ab3bf89; Illinois Opens Blockchain Development Partnership with Hashed Health, The Illinois Blockchain Initiative (Aug. 9, 2017), available at https://illinoisblockchain.tech/illinois-opens-blockchain-development-partnership-with-hashed-health-fe3891e500bb; IDFPR Joins R3 Consortium, The Illinois Blockchain Initiative (July 20, 2017), available at https://illinoisblockchain.tech/idfpr-joins-r3-consortium-390e2d6f6adb.

92 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, Release: PR7231-15 (Sept. 17, 2015), http://www.cftc.gov/PressRoom/PressReleases/pr7231-15 (hereinafter, "Coinflip Settlement").

93 See generally Commodity Exchange Act, 49 Stat. 1491, 7 U.S.C. §§ 1, et seq.

94 7 U.S.C. § 1a(9).

95 See, e.g., U.S. Commodity Futures Trading Commission, Testimony of Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition & Forestry (Dec. 10, 2014), available at http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6.

96 Coinflip Settlement.

97 LedgerX, LLC, Order of Registration, July 6, 2017, available at http://www.cftc.gov/PressRoom/PressReleases/pr7584-17; LedgerX, LLC Order of Registration, July 24, 2017, available at http://www.cftc.gov/idc/groups/public/@otherif/documents/ifdocs/ledgerxdcoregorder72417.pdf.

98 http://www.cftc.gov/PressRoom/PressReleases/pr7654-17

99 http://www.cftc.gov/LabCFTC/index.htm

100 31 C.F.R. § 1010.100(ff).

101 31 C.F.R. § 1010.100(ff)(5)(i)(A) (emphasis added).

102 U.S. Department of the Treasury, FinCEN, BSA Requirements for MSBs, https://www.fincen.gov/financial_institutions/msb/msbrequirements.html.

103 18 U.S.C. § 1960.

104 U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013), available at https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

105 Id.

106 U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Virtual Currency Mining Operations, FIN-2014-R001 (Jan. 30, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R001.html.

107 U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013), available at https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

108 U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Virtual Currency Mining Operations, FIN-2014-R001 (Jan. 30, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R001.html.

109 U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity, FIN-2014-R002 (Jan. 30, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R002.html.

110 U.S. Department of the Treasury, FinCEN, Application of Money Services Business regulations to the rental of computer systems for mining virtual currency, FIN-2014-R007 (Apr. 29, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R007.html.

111 U.S. Department of the Treasury, FinCEN, Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform , FIN-2014-R011 (Oct. 27, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R011.html.

112 Id.

113 U.S. Department of the Treasury, FinCEN, Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, FIN-2014-R012 (Oct. 27, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R012.html.

114 U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Persons Issuing Physical or Digital Negotiable Certificates of Ownership of Precious Metals, FIN-2015-R001 (Aug. 14, 2015), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2015-R001.html.

115 Office of the Comptroller of the Currency, Exploring Special Purpose National Bank Charters for Fintech Companies (Dec. 2016), available at https://www.occ.treas.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf.

116 Id.

117 Id.

118 Office of the Comptroller of the Currency, Comptroller's Licensing Manual Draft Supplement: Evaluating Charter Applications from Financial Technology Companies (Mar. 2017), available at https://www.occ.gov/publications/publications-by-type/licensing-manuals/file-pub-lm-fintech-licensing-manual-supplement.pdf.

119 Id.

120 Id.

121 Office of the Comptroller of the Currency, Exploring Special Purpose National Bank Charters for Fintech Companies

(Dec. 2016), available at https://www.occ.treas.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf.

122 See, e.g., Perianne Boring, You Down with OCC? – FinTech Firms See Promise in Special Bank Charter, Forbes (Jan. 27, 2017), https://www.forbes.com/sites/perianneboring/2017/01/27/you-down-with-occ-fintech-firms-see-promise-in-special-bank-charter/#78ad48db32e1.

123 Letter from Maria T. Vullo, Superintendent of the New York State Department of Financial Services to Thomas J. Curry, Comptroller of the Office of the Comptroller of the Currency (Jan. 17, 2017), available at http://www.dfs.ny.gov/about/occ_letter1-17-17.pdf.

124 Complaint for Declaratory and Injunctive Relief, Conference of State Bank Supervisors v. Office of the Comptroller of the Currency, Civ. Act. No. 1:17-cv-00763 (D.D.C. Apr. 26, 2017), available at https://bankcsbs.files.wordpress.com/2017/04/csbs-occ-complaint-final.pdf.

125 Complaint for Declaratory and Injunctive Relief, Vullo v. Office of the Comptroller of the Currency, Civ. Act. No. 1:17-cv-03574 (S.D.N.Y. May 12, 2017), available at http://www.dfs.ny.gov/about/ea/ea170512.pdf.

126 U.S. Securities and Exchange Commission, Self-Regulatory Organizations; Bats BZX Exchange, Inc.; Order Disapproving a Proposed Rule Change, as Modified by Amendments No. 1 and 2, to BZX Rule 14.11(e)(4), Commodity-Based Trust Shares, to List and Trade Shares Issued by the Winklevoss Bitcoin Trust (Mar. 10, 2017), https://www.sec.gov/rules/sro/batsbzx/2017/34-80206.pdf.

127 Id. at 2.

128 Id.

129 Id.

130 Id. at 38.

131 U.S. Securities and Exchange Commission, Self-Regulatory Organizations; NYSE Arca, Inc.; Order Disapproving a Proposed Rule Change, as Modified by Amendment No. 1, Relating to the Listing and Trading of Shares of the SolidX Bitcoin Trust under NYSE Arca Equities Rule 8.201 (Mar. 28, 2017), https://www.sec.gov/rules/sro/nysearca/2017/34-80319.pdf.

132 Arjun Kharpal, Bitcoin marches towards all-time high as SEC gives potential second shot to Winklevoss ETF, CNBC (Apr. 26, 2017), http://www.cnbc.com/2017/04/26/bitcoin-price-sec-winklevoss-etf-review.html.

133 Id.; Reuters, Why Bitcoin Investors Are Increasingly Optimistic About SEC Approval, Fortune Tech (Mar. 3, 2017), http://fortune.com/2017/03/03/bitcoin-pricing-record/; Laura Shin, SEC Rejects Winklevoss Bitcoin ETF, Sending Price Tumbling, Forbes (Mar. 10, 2017), https://www.forbes.com/sites/laurashin/2017/03/10/sec-rejects-winklevoss-bitcoin-etf-sending-price-tumbling/#31af4fa3643c.

134 SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities, SEC Release 2017-131, available at https://www.sec.gov/news/press-release/2017-131; SEC Exercises Jurisdiction over Initial Coin Offerings, July 27, 2017, available at https://www.reedsmith.com/en/perspectives/2017/07/sec-exercises-jurisdiction-over-initial-coin-offerings.

135 SEC Release No. 81367, Aug. 9, 2017, available at https://www.sec.gov/litigation/suspensions/2017/34-81367.pdf.

136 SEC Release No. 81474, Aug. 23, 2017, available at https://www.sec.gov/litigation/suspensions/2017/34-81474.pdf.

137 In the Matter of American Security Resources Corp., File No. 500-1 (Aug. 24, 2017), available at https://www.sec.gov/litigation/suspensions/2017/34-81481-o.pdf.

138 https://www.sec.gov/news/press-release/2017-176

139 Internal Revenue Service, IRS Virtual Currency Guidance : Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply, IR-2014-36 (Mar. 25, 2014), https://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance.

140 Treasury Inspector General for Tax Administration, Final Audit Report – As the Use of Virtual Currencies in Taxable Transactions Becomes More Common, Additional Actions Are Needed to Ensure Taxpayer Compliance (Audit # 201530022), Reference Number: 2016-30-083 (Sept. 21, 2016), https://www.treasury.gov/tigta/auditreports/2016reports/201630083fr.pdf.

141 Kelly Phillips Erb, IRS Wants Court Authority to Identify Bitcoin Users & Transactions at Coinbase, Forbes (Nov. 21, 2016), https://www.forbes.com/sites/kellyphillipserb/2016/11/21/irs-wants-court-authority-to-identify-bitcoin-users-transactions-at-coinbase/#2ac6c1055979.

142 26 U.S.C. § 7609(f)(2).

143 FINRA, Distributed Ledger Technology: Implications of Blockchain for the Securities Industry (Jan. 2017), available at http://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf.

144 Consumer Financial Protection Bureau, Consumer Advisory: Risks to Consumers Posed by Virtual Currency (Aug. 2014), http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf.

145 Bureau of Consumer Financial Protection, Final Rule: Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z), 81 Fed. Reg. 83934, 83978 (Nov. 22, 2016).

146 In the Matter of Coinflip, Inc., et al., Comm. Fut. L. Rep. (CCH) ¶33,538, (Sep. 17, 2015).

147 U.S. Commodity Futures Trading Commission, CFTC Orders Bitcoin Exchange Bitfinex to Pay $75,000 for Offering Illegal Off-Exchange Financed Retail Commodity Transactions and Failing to Register as a Futures Commission Merchant, Release: pr7380-16 (June 2, 2016), http://www.cftc.gov/PressRoom/PressReleases/pr7380-16.

148 CFTC v. Gelfman Blueprint, Inc. and Nicholas Gelfman, Case No. 17-7181 (S.D. N.Y. 2017) (CFTC filed complaint against defendants for operating a bitcoin Ponzi scheme).

149 U.S. Department of the Treasury, FinCEN, FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger (May 5, 2015), https://www.fincen.gov/news_room/nr/html/20150505.html.

150 https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-11 0-million-facilitating-ransomware

151 U.S. Securities and Exchange Commission, Final Judgment Entered Against Trendon T. Shavers, A/K/A/ "Pirateat40" - Operator of Bitcoin Ponzi Scheme Ordered to Pay More Than $40 Million in Disgorgement and Penalties, Litigation Release No. 23090 (Sept. 22, 2014), https://www.sec.gov/litigation/litreleases/2014/lr23090.htm.

152 U.S. Securities and Exchange Commission, SEC Sanctions Operator of Bitcoin-Related Stock Exchange for Registration Violations, Press Release 2014-273 (Dec. 8, 2014), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370543655716.

153 U.S. Securities and Exchange Commission, SEC Charges Bitcoin Entrepreneur With Offering Unregistered Securities, Press Release 2014-111 (June 3, 2014), http://

www.sec.gov/News/PressRelease/Detail/PressRelease/1370541972520.

154 U.S. Securities and Exchange Commission, Release 2015-271, SEC Charges Bitcoin Mining Companies (Dec. 1, 2015), https://www.sec.gov/news/pressrelease/2015-271.html.

155 Stan Higgins, Bitcoin Investment Trust and Genesis Trading Settle With SEC, CoinDesk (July 11, 2016), http://www.coindesk.com/bitcoin-investment-trust-50000-settlement/.

156 https://www.reedsmith.com/en/perspectives/2017/10/sec-enforcement-action-involving-initial-coin-offering

157 https://www.sec.gov/litigation/complaints/2017/compr2017-219.pdf; https://www.sec.gov/litigation/admin/2017/33-10445.pdf

158 U.S. Attorney's Office for the Southern District of New York, Press Release: Ross Ulbricht, aka Dread Pirate Roberts, Sentenced in Manhattan Federal Court to Life in Prison (May 29, 2015), https://www.fbi.gov/newyork/press-releases/2015/ross-ulbricht-aka-dread-pirate-roberts-sentenced-in-manhattan-federal-court-to-life-in-prison.

159 U.S. Attorney's Office for the Southern District of New York, Press Release: Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court (Nov. 6, 2014), https://www.fbi.gov/newyork/press-releases/2014/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court.

160 U.S. Attorney's Office for the Southern District of New York, Press Release: Bitcoin Exchanger Sentenced In Manhattan Federal Court To Four Years In Prison For Selling Nearly $1 Million In Bitcoins For Drug Buys On Silk Road (Jan. 20, 2015), http://www.justice.gov/usao-sdny/pr/bitcoin-exchanger-sentenced-manhattan-federal-court-four-years-prison-selling-nearly-1.

International regulatory landscape

161 https://www.reedsmith.com/en/perspectives/2017/09/the-fca-offers-its-two-cents-on-initial-coin-offerings.

162 Case C-264/14, Skatteverket v. David Hedqvist (Oct. 22, 2015), available at http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d-2dc30dd8ccd881260ee4096a4a6a9b3d479002e.e34KaxiLc3qMb40Rch0SaxuRbxn0?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=170305&occ=first&dir=&cid=854516 ("ECJ Ruling").

163 See infra, III.B.1

164 ECJ Ruling.

165 Digits: Tech News & Analysis from the WSJ, EU Rules Bitcoin Is a Currency, Not a Commodity—Virtually (Oct. 22, 2015), http://blogs.wsj.com/digits/2015/10/22/eu-rules-bitcoin-is-a-currency-not-a-commodity-virtually/.

166 http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2016-009012&language=EN

167 http://blogs.ec.europa.eu/eupolicylab/files/2017/04/Blockchain4EU_Kickoff-announcement.pdf

168 https://ec.europa.eu/digital-single-market/en/news/pre-information-notice-eu-blockchain-observatory-forum

169 https://www.esma.europa.eu/press-news/esma-news/esma-assesses-dlt%E2%80%99s-potential-and-interactions-eu-rules

170 European Banking Authority, EBA Opinion on 'virtual currencies,' EBA/Op/2014/08 (July 4, 2014), available at https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

171 Id. at 5.

172 Id.

173 Id.

174 https://www.ecb.europa.eu/pub/annual/special-features/2016/html/index.en.html and https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf

175 https://www.reuters.com/article/us-blockchain-ecb/blockchain-immature-for-big-central-banks-ecb-and-boj-say-idUSKCN1BH2DH

176 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0849&cm_mid=5848746&cm_crmid=8a7e8047-5fb8-e511-87f4-0050569f4bf8&cm_medium=email

177 The Legislative Decree No. 90 of 25 May 2017.

178 https://www.jerseylaw.je/laws/enacted/Pages/RO-099-2016.aspx

179 Sarah Jane Hughes and Stephen T. Middlebrook, Advancing a Framework for Regulating Virtual Currency Payments Intermediaries, 32 Yale J. Reg. 496 (2015); Merkle Tree, http://merkletree.io.

180 Robleh Ali, John Barrdear, Roger Clews and James Southgate, Bank of England Quarterly Bulletin 2014 Q3, Innovations in payment technologies and the emergence of digital currencies, http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf.

181 http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf

182 State Secretariat for International Financial Matters SIF, Federal Council publishes report on virtual currencies such as bitcoin (June 25, 2014), https://www.sif.admin.ch/sif/en/home/dokumentation/medienmitteilungen/medienmitteilungen.msg-id-53513.html.

183 https://www.theguardian.com/technology/2017/jul/31/cryptocurrencies-more-investment-way-pay-bitcoin-regulation

184 Central Bank of Iceland, Significant risk attached to use of virtual currency (Mar. 19, 2014), http://www.cb.is/publications-news-and-speeches/news-and-speeches/news/2014/03/19/Significant-risk-attached-to-use-of-virtual-currency/.

185 https://bitcoinist.com/bitcoin-still-illegal-six-countries/

186 https://www.fca.org.uk/publications/discussion-papers/dp17-3-discussion-paper-distributed-ledger-technology

187 https://www.fca.org.uk/news/speeches/our-role-promoting-innovation

188 https://www.fca.org.uk/news/press-releases/financial-conduct-authority-provides-update-regulatory-sandbox

189 https://www.reedsmith.com/en/perspectives/2017/06/fca-releases-discussion-paper-on-distributed-ledger-technology

190 https://www.fca.org.uk/news/statements/initial-coin-offerings

191 https://www.sif.admin.ch/sif/en/home/dokumentation/medienmitteilungen/medienmitteilungen.msg-id-53513.html

192 Why Bangladesh will jail Bitcoin traders, The Telegraph (Sep. 15, 2014), http://www.telegraph.co.uk/finance/currency/11097208/Why-Bangladesh-will-jail-Bitcoin-traders.html.

193 China Central Bank Warns Banks on Bitcoin, Wall Street Journal (May 7, 2014), http://www.wsj.com/articles/SB10001424052702304655304579547251552490962; Alex Hern, Bitcoin price tumbles after warning from Chinese central bank, The Guardian (Dec. 5, 2013), http://www.theguardian.com/technology/2013/dec/05/bitcoin-price-tumbles-chinese-central-bank-warning.

194 Pathom Sangwongwanich, Bitcoins back in the Thai marketplace, Bangkok Post (Feb. 20, 2014), http://www.bangkokpost.com/business/marketing/395952/bitcoins-back-in-the-thai-marketplace.

195 Japan's ruling party says won't regulate bitcoin for now, Reuters (June 19, 2014), http://www.reuters.com/article/2014/06/19/japan-bitcoin-idUSL4N0P01LS20140619.
196 http://www.reuters.com/article/us-southkorea-bitcoin/south-korea-bans-raising-money-through-initial-coin-offerings-idUSKCN1C408N
197 Virtual Currencies: International Actions and Regulations, Perkins Coie (last updated Oct. 2015), https://www.perkinscoie.com/en/news-insights/virtual-currencies-international-actions-and-regulations.html#Japan.
198 Christine Duhaime, Canada implements world's first national digital currency law; regulates new financial technology transactions, Duhaime Law Notes (June 22, 2014, updated July 30, 2014), http://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law/
199 Id.
200 Id.
201 Id.
202 Stan Higgins, Ecuador Bans Bitcoin, Plans Own Digital Money, CoinDesk (July 25, 2014), http://www.coindesk.com/ecuador-bans-bitcoin-legislative-vote/; Jim Wyss, Ecuador's new virtual currency is a source of pride, worry, Miami Herald (Aug. 12, 2015), http://www.miamiherald.com/news/nation-world/world/americas/article30968391.html.
203 Id.
204 Pete Rizzo, Bolivia's Central Bank Bans Bitcoin, CoinDesk (June 19, 2014), http://www.coindesk.com/bolivias-central-bank-bans-bitcoin-digital-currencies/.
205 Hughes and Middlebrook; Merkle Tree.
206 https://bitcoinmagazine.com/articles/bitcoin-exempt-uae-central-banks-ban-virtual-currencies/
207 https://news.bitcoin.com/uae-not-ban-bitcoin/
208 https://www.coindesk.com/dubai-government-ibm-city-blockchain-pilot/
209 https://cointelegraph.com/news/united-arab-emirates-consider-to-officially-recognize-bitcoin-work-on-regulatory-framework
210 https://www.e-marmore.com/MarMore/media/TOCDownloadPDF/Bitcoins-ExecSummary.pdf
211 http://news.kuwaittimes.net/website/bitcoin-gaining-popularity-in-kuwait/
212 http://vision2030.gov.sa/sites/default/files/NTP_En.pdf
213 https://www.coindesk.com/saudi-uae-central-banks-team-test-cryptocurrency/
214 http://www.newsofbahrain.com/viewNews.php?pId=38219&pid=21&MNU=
215 https://www.coindesk.com/qatars-commercial-bank-unveils-blockchain-remittance-pilot/
216 https://www.coindesk.com/israel-may-gearing-tax-bitcoin-kind-property/
217 https://www.bitsofgold.co.il
218 https://news.bitcoin.com/banks-deny-service-bitcoin-businesses-israel/
219 See Merkle Tree.
220 Farhaanah Mahomed, S.African Financial Authorities Warn Against Virtual Currencies, CNBC Africa (Feb. 12, 2015), http://www.cnbcafrica.com/news/southern-africa/2014/09/18/virtual-currencies-warning/.
221 Id.
222 https://news.bitcoin.com/south-africa-will-begin-testing-bitcoin-and-cryptocurrency-regulations/
223 https://www.moneyweb.co.za/news/tech/south-africa-open-to-digital-currency/
224 http://ftreporter.com/tunisia-is-the-first-country-to-put-national-currency-on-blockchain/

Insuring digital currency and digital currency business

225 In this chapter, references to "bitcoin" generally also refer to similar derivative cryptocurrencies.
226 SEC v. Shavers, No. 4:13CV416, 2013 WL 4028182, at *2 (E.D. Tex. Aug. 6, 2013).
227 Internal Revenue Service, IRS Virtual Currency Guidance : Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply, IR-2014-36 (Mar. 25, 2014), https://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance
228 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, Release: PR7231-15 (Sept. 17, 2015), http://www.cftc.gov/PressRoom/PressReleases/pr7231-15 (hereinafter, "Coinflip Settlement")
229 For example, virtual currency has been banned outright in Ecuador and Bolivia (although the Ecuadorian government has created its own state-backed digital currency). In China, the use of Bitcoin and virtual currencies is technically legal, but steps by the Chinese government and regulators to restrict the use of bitcoin have made the use of such currencies difficult if not impossible. See Bitcoin in China: A dream dispelled, Chinese regulators make life hard for crypto-currencies, The Economist, Apr. 12, 2014, available at http://www.economist.com/news/finance-and-economics/21600736-chinese-regulators-make-life-hard-crypto-currencies-dream-dispelled.
230 See Chapters 5 & 7 of this White Paper, discussing security concerns particular to bitcoin; see also Lloyd's Bitcoin Report.
231 Hannover Group has modified its commercial crime policy by endorsement to include "Bitcoins" in its definition of "Money." See Bitpay, Inc. v. Massachusetts Bay Ins. Co., No. 1:15-cv-03238 (N.D. Ga.) (Ex. A to Bitpay's compl., at Doc. 1-1, Manuscript End. 1).
232 See Press Release, "Great American Insurance Group First to Offer Bitcoin Coverage to Commercial and Governmental Entities," available at http://www.businesswire.com/news/home/20140602006331/en/Great-American-Insurance-Group-Offer-Bitcoin-Coverage (last visited Oct. 16, 2015).
233 Commercial Crime Policy form (ISO 2015), §D(1)(k).
234 "Include Virtual Currency as Money Endorsement," Form CR 25 45 11 15 (ISO 2015).
235 Bitpay, Inc. v. Massachusetts Bay Ins. Co., No. 1:15-cv-03238 (N.D. Ga.).
236 See, e.g. Medidata Solutions, Inc. v. Fed. Ins. Co., 2017 WL 3268529 (S.D.N.Y. July 21, 2017) (coverage under computer fraud and funds transfer fraud insuring agreements of commercial crime policy because of sufficient nexus between fraudulent use of a computer and the loss); Principle Solutions Group, LLC v. Ironshore Indemnity, Inc., 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016) (scheme involving fraudulent emails designed to look like they came from the company's president was covered under commercial crime policy's computer fraud provision); But see Taylor & Lieberman v. Fed. Ins. Co., 681 F. App'x 627 (9th Cir. 2017) (neither the Computer Fraud nor the Funds Transfer Fraud

insuring agreements of a crime policy applied to provide coverage for a social engineering fraud) ; Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252 (5th Cir. 2016) (loss resulting from a fraudulent email did not trigger coverage under a crime policy's "computer fraud" coverage because the loss was not the "direct result" of computer use); Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017) (same).

237 See, e.g., https://www.beazley.com/usa/specialty_lines/professional_liability/technology_media_and_business_services/fidelity_and_crime.html (last visited Sept. 19, 2017); https://www2.chubb.com/us-en/business-insurance/social-engineering-fraud-coverage-for-crime-insurance.aspx (last visited Sept. 19, 2017).

238 See https://www.bitgo.com/insurance (last visited Oct. 16, 2015).

239 See supra, Note 8.

240 See https://support.xapo.com/insurance (last visited Oct. 7, 2015).

Applications in capital markets

241 See, e.g., Nathaniel Popper, Bitcoin Technology Piques Interest on Wall St., New York Times DealBook (Aug. 28, 2015), http://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html?_r=0.

242 Edward Robinson and Matthew Leising, Blythe Masters Tells Banks the Blockchain Changes Everything, BloombergBusiness (Aug. 31, 2015), http://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything; Jemima Kelly, Nine of world's biggest banks join to form blockchain partnership, Reuters (Sept. 15, 2015), http://www.reuters.com/article/2015/09/15/us-banks-blockchain-idUSKCN0RF24M20150915#vbbT0RlRCTT8TkRP.97.

243 Accenture, Blockchain in the Investment Bank (2015), available at https://www.accenture.com/t20150811T015521__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_13/Accenture-Blockchain-Investment-Bank.pdf#zoom=50.

244 Nathaniel Popper, Bitcoin Technology Piques Interest on Wall St., New York Times DealBook (Aug. 28, 2015), http://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html?_r=0.

245 https://www.greenwich.com/greenwich-research/research-documents/greenwich-reports/2015/jul/is-digital-ledger-tech-2015-gr

246 https://www.greenwich.com/fixed-income-fx-cmds/blockchain-adoption-capital-markets

247 http://www.efinancialnews.com/story/2015-09-10/capital-markets-blockchain-spend-to-reach-400-million-by-2019

248 See, e.g., Joanna Payne, Stock Settlement: Why You Need to Understand the T+3 Timeline, Charles Schwab (May 21, 2014), http://www.schwab.com/public/schwab/nn/articles/Stock-Settlement-Why-You-Need-to-Understand-the-T-3-Timeline.

249 See, e.g., Kristen Haunss, LPC: Loan Market Pushes Forward to Cut Settlement Times,Reuters (May 12, 2016), http://www.reuters.com/article/us-loan-settlement-idUSKCN0Y323YI.

250 Nasdaq, Article: How Stock Exchanges are Experimenting with Blockchain Technology (June 12, 2017), http://www.nasdaq.com/article/how-stock-exchanges-are-experimenting-with-blockchain-technology-cm801802.

251 Id.

252 http://www.reuters.com/article/us-dtcc-blockchain-repos/dtcc-completes-blockchain-repo-test-idUSKBN1661L9.

253 http://www.dtcc.com/news/2016/april/07/successful-blockchain-test-completed.

254 http://www.coindesk.com/european-banks-select-ibm-blockchain-small-business-platform/.

255 Experian, Article: Does Valid Bank Account Data Matter? A guide to payments globally: How payment failures can be reduced through managing bank account date. https://www.experian.co.uk/assets/payments/international-payments-guide.pdf.

256 https://techcrunch.com/2017/05/23/wtf-is-an-ico/.

257 https://www.coindesk.com/ico-tracker/.

258 https://www.coindesk.com/bitcoin-venture-capital/.

259 https://www.ethnews.com/status-completes-token-offering-raises-roughly-90-million-dollars.

260 https://qz.com/1004892/the-bancor-ico-just-raised-153-million-on-ethereum-in-three-hours/.

261 https://www.forbes.com/sites/omribarzilay/2017/07/15/tezos-232-million-ico-may-just-be-the-beginning/#13aa9c304c52.

262 https://www.cryptocoinsnews.com/filecoin-ico-raises-record-250-million-from-accredited-investors/.

263 https://www.coindesk.com/kik-ico-raises-98-million-but-falls-short-of-target/.

264 Strategy&, Article: Considering an IPO? The costs of going and being public may surprise you (September 2012), https://www.strategyand.pwc.com/media/file/Strategyand_Considering-an-IPO.pdf.

265 https://coinmarketcap.com/.

266 https://www.valuewalk.com/2017/08/cryptocurrency-hedge-funds-bitcoin-price/.

267 Id.

268 15 U.S.C. §§ 77b(a)(1); 78d.

269 See SEC v. W.J.. Howey Co., 328 U.S. 293, 299 (1946) (noting that the term "investment contract" is flexible and captures "countless and variable schemes devised by those who seek to use the money of others on the promise of profits").

270 United Hous. Found., Inc. v. Forman, 421 U.S. 837, 852 (1975).

271 15 U.S.C. §§ 77e(a); 77e(c).

272 See Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, SEC Release No. 81207 (July 25, 2017).

273 Id. at 10.

274 http://www.cftc.gov/PressRoom/PressReleases/pr7631-17#PrRoWMBL

275 http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx

276 https://www.fca.org.uk/news/statements/initial-coin-offerings.

277 https://www.coindesk.com/hong-kong-regulator-warns-ico-tokens-may-securities/.

278 https://www.coindesk.com/asic-on-blockchain-australias-securities-watchdog-unlikely-to-regulate-icos.

279 http://www.osc.gov.on.ca/documents/en/Securities-Category4/csa_20170824_cryptocurrency-offerings.pdf.

280 https://www.securities-administrators.ca/aboutcsa.aspx-

?id=1555.

281 https://www.coindesk.com/ico-ban-canadas-regulators-giving-one-token-sale-big-break/.

282 https://www.coindesk.com/china-outlaws-icos-financial-regulators-order-halt-token-trading/.

283 http://www.telegraph.co.uk/technology/2017/08/01/bitcoin-cash-everything-need-know-bitcoins-hard-fork/.

284 https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/.

285 https://cointelegraph.com/news/ethereum-hard-fork-no-4-has-arrived-as-dos-attacks-intensify.

Blockchain innovation in the energy, commodities, shipping and trade finance industries

286 There is evidence to suggest that rice futures were traded in Ancient China as early as 6000 B.C.

287 https://www.ft.com/content/7928cdaa-f07e-11e3-8f3d-00144feabdc0

288 http://www-03.ibm.com/press/us/en/pressrelease/51951.wss

289 https://www.brooklyn.energy/

290 http://www.cryptomudra.com/2017/09/power-ledger-introduces-decentralized-peer-peer-energy-transfer-network/

291 https://www.elexon.co.uk/bsc-and-codes/balancing-settlement-code/

292 https://www.economist.com/news/leaders/21717371-thats-no-reason-governments-stop-supporting-them-wind-and-solar-power-are-disrupting

293 https://www.ofgem.gov.uk/data-portal/average-switching-time-domestic-customers-gb

294 https://www.ofgem.gov.uk/publications-and-updates/moving-reliable-next-day-switching-consultation-target-operating-model-and-delivery-approach

295 https://techcrunch.com/2016/12/13/electron-is-trying-to-sell-a-blockchain-makeover-to-the-uks-energy-sector/

296 Regulation (EU) No 1227/2011 of the European Parliament and of the council of 25 October 2011 on wholesale energy market integrity and transparency.

297 In the same manner as ISDA is considering for derivatives transactions https://www.lexology.com/library/detail.aspx-?g=d8c187cb-dc73-4518-b3b5-930d56cbd5c3

298

299 Bilur FAQs, https://www.bilurmarket.com/faqs.

300 Press Release: European Energy Trading Firms test peer-to-peer Trading over the Blockchain, May 29, 2017, available at https://enerchain.ponton.de/index.php/articles/2-uncategorised/21-enerchain-p2p-trading-project.

301 IEEE Spectrum, Will Energy Offer the Next Market for Blockchain? May 17, 2017, available at http://spectrum.ieee.org/energywise/energy/the-smarter-grid/will-energy-offer-the-next-market-for-blockchain.

302 Reuters, Mercuria introduce blockchain to oil trade with ING, SocGen, Jan. 19, 2017, available at http://www.reuters.com/article/us-davos-meeting-mercuria-idUSKBN1531DJ.

303 Finextra, IBM, Natixis and Trafigura team on blockchain platform for oil trades, Mar. 28, 2017, available at https://www.finextra.com/newsarticle/30350/ibm-natixis-and-trafigura-team-on-blockchain-platform-for-oil-trades.

304 ISDA, Smart Contracts and Distributed Ledger – A Legal Perspective, Aug. 2017, available at https://www2.isda.org/attachment/OTU3MQ==/Smart%20Contracts%20and%20Distributed%20Ledger%20%20A%20Legal%20Perspective.pdf.

305 https://www.finextra.com/blogposting/13102/blockchain-financial-regulatory-reporting-and-challenges

306 One study showed that even simple shipments can involve 30 parties and more than 200 communications between them. Reuters, IBM, Maersk in blockchain tie-up for shipping industry, 6 March 2017, available at: http://www.reuters.com/article/us-usa-blockchain-ibm/ibm-maersk-in-blockchain-tie-up-for-shipping-industry-idUSKBN16D26Q

307 Opensea.pro, How Can the Shipping Industry Take Advantage of the Blockchain Technology? available at https://opensea.pro/blog/blockchain-for-shipping-industry

308 John Southurst, "How Blockchain Contracts and IoT Could Save Global Shipping Billions," Bitcoin News (Nov. 10, 2016), available at https://news.bitcoin.com/blockchain-save-global-shipping-billions/

309 Reuters, IBM, Maersk in blockchain tie-up for shipping industry, 6 March 2017, available at: http://www.reuters.com/article/us-usa-blockchain-ibm/ibm-maersk-in-blockchain-tie-up-for-shipping-industry-idUSKBN16D26Q

310 Ship-technology.com, Could blockchain technology revolutionise shipping?, available at: http://www.ship-technology.com/features/featurecould-blockchain-technology-revolutionise-shipping-5920391/

311 Linex Systems, HMM completes first blockchain pilot voyage, 7 September 2017, available at: https://ca.linexsystems.com/contents/transit/2048225065?user_id=815745&log=6719bcf9c34cde1ac6b390b56d263d79&p=52918035&m=1&s=213975&org_id=390345

312 http://fortune.com/2017/08/22/walmart-blockchain-ibm-food-nestle-unilever-tyson-dole/

313 https://www.reedsmith.com/en/perspectives/2016/01/electronic-bills-of-lading-another-step-forward

314 Financial Time, Moller-Maersk puts cost of cyber attack at up to $300m, 16 August 2017, avialble at: https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff and marinemec.com, Blockchain would have prevented Maersk cyber attack, 30 June 2017, available at: http://www.marinemec.com/news/view,blockchain-would-have-prevented-maersk-cyber-attack_48287.htm

315 Financial Times, Marine insurers adopt blockchain contracts , 6 September 2017, available at: https://www.ft.com/content/d7e08624-918b-11e7-a9e6-11d2f0ebb7f0

316 ibid.

317 Blockchain.com, EY, Guardtime And Industry Participants Launch The World's First Marine Insurance Blockchain Platform, 8 September 2017, available at: http://www.the-blockchain.com/2017/09/08/ey-guardtime-industry-participants-launch-worlds-first-marine-insurance-blockchain-platform/

318 Opensea.pro, How Can the Shipping Industry Take Advantage of the Blockchain Technology? available at https://opensea.pro/blog/blockchain-for-shipping-industry.

319 Sanne Wass, "Landmark transaction merges blockchain, smart contracts and IoT," Global Trade Review (Oct. 23, 2016), available at https://www.gtreview.com/news/global/landmark-transaction-merges-blockchain-smart-contracts-and-iot/.

320 "The Benefits and Limitation of Smart Contracts in Trade and Supply Chain," Commonwealth Bank of Australia (Feb. 2, 2017), available at https://www.commbank.com.au/guidance/blog/the-benefits-and-limitations-of-smart-contracts-in-trade-and-sup-201701.html.

321 Id. "There are so many rights, options and abilities in com-

mercial transactions that it isn't realistic to write a logic path that entirely covers the relationship. The automated logic path should be used when it is most efficient, and human discretion and judgment should be used in other circumstances. That would make a really 'smart' contract."

322 The blockchain revolution in trade finance https://www.barclayscorporate.com/insight-and-research/trading-and-exporting/blockchain-revolution-in-trade-finance.html

323 Digital Trade Chain, 7 Banks Could go Live with Blockchain in 2017 https://www.coindesk.com/digital-trade-chain-banks-blockchain-2017/

324 Bringing trade finance to small and medium enterprises, IBM, June 27, 2017, https://www.ibm.com/blogs/blockchain/2017/06/bringing-trade-finance-to-small-and-medium-enterprises/

325 Barclays and Wave complete world's first blockchain trade finance transaction, Financial Times, 07 Sep 2016, http://www.newsroom.barclays.com/r/3396/barclays_and_wave_complete_world_first_blockchain_trade#

326 Will blockchain make trade finance banks redundant? GTR Global Trade Review 14-06-17 / by Finbarr Bermingham https://www.gtreview.com/news/global/will-blockchain-make-trade-finance-banks-redundant/

327 Streamlining Trade Finance With Blockchain Technology By Phillip Silitschanuhttps://www.americanexpress.com/us/content/foreign-exchange/articles/blockchain-technology-to-streamline-trade-finance/

328 European banks to launch blockchain trade finance platform, Financial Times, June 26, 2017, https://www.ft.com/content/6bb4f678-5a8c-11e7-b553-e2df1b0c3220

329 http://www.ibtimes.co.uk/hsbc-bank-america-merrill-lynch-use-hyperledger-project-blockchain-based-trade-finance-1575269

330 Banks bring blockchain innovation to letters of credit 10-08-16 / by Sofia Lotto Persio https://www.gtreview.com/news/asia/banks-blockchain-innovation-letters-of-credit/

331 Banks' blockchain consortium picks IBM for trade finance platform, Jemima Kelly, 26 June 2017. https://uk.reuters.com/article/us-banks-blockchain-ibm-idUKKBN19H2M6

Privacy and re-identification on the blockchain

332 Privacy-enhancing technologies for the Internet, Ian Goldberg, David Wagner, Eric Brewer, University of California, Berkeley (1997), available at https://www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html.

333 Id.

334 How Anonymous is Bitcoin? A Backgrounder for Policymakers, Adam Ludwin (January 25, 2015), available at http://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/.

335 The promise of managing identity on the blockchain (September 10, 2017) available at https://techcrunch.com/2017/09/10/the-promise-of-managing-identity-on-the-blockchain/

336 Id.

337 How Anonymous is Bitcoin? A Backgrounder for Policymakers, Adam Ludwin (January 25, 2015), available at http://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/.

338 The promise of managing identity on the blockchain (September 10, 2017) available at https://techcrunch.com/2017/09/10/the-promise-of-managing-identity-on-the-blockchain/

339 https://z.cash/technology/index.html

340 DRAFT NISTIR 8053 1, De-Identification of Personally Identifiable Information, Simon L. Garfinkel, National Institute of Standards and Technology, U.S. Department of Commerce (April 2015) ("Deidentification Standards"), p. 5.

341 Deidentification Standards, p. 6.

342 Id.

343 Id. at 17.

344 Deidentification Standards, p. 17.

345 Opinion 05/2014 on Anonymisation Techniques, Article 29 Working Group (Adopted 10 April 2014), p. 5.

346 Id. at 17.

347 Id. at 22.

348 Id.

349 Unravelling the mystery of blockchain – Should privacy professionals be concerned? (July 28, 2016) available at https://iapp.org/news/a/unravelling-the-mystery-of-blockchain-should-privacy-professionals-be-concerned/

350 Blockchain and big data privacy in healthcare (May 2, 2016) available at https://iapp.org/news/a/blockchain-and-big-data-privacy-in-healthcare/

351 https://pokitdok.com/security/

352 PokitDok teams with Intel on healthcare blockchain solution (May 10, 2017) available at https://techcrunch.com/2017/05/10/pokitdok-teams-with-intel-on-healthcare-blockchain-solution/

353 Why J.P. Morgan Chase Is Building a Blockchain on Ethereum (October 04, 2016) available at http://fortune.com/2016/10/04/jp-morgan-chase-blockchain-ethereum-quorum/

354 Solving Blockchain's Privacy Problem (July 31, 2017) available at http://www.newsweek.com/solving-blockchain-privacy-problem-643368

355 Id.

356 How Banks Will Stop Snoops From Using the Blockchain to Front-Run Trades (July 07, 2016) available at http://fortune.com/2016/07/07/blockchain-r3/

Intellectual property

357 https://bitcoin.org/en/

358 https://github.com/ethereum/wiki/wiki/Licensing

359 https://litecoin.org/

360 https://github.com/openchain/openchain/blob/master/LICENSE

361 https://opensource.org/licenses/mit-license.php

362 https://www.hyperledger.org/about/charter

363 Id.

364 © Questel Orbit 2017, reproduced with permission. Questel analysis and images in this chapter were prepared by Daniela Hoyos, Analyst at Questel Consulting.

365 © Questel Orbit 2017, reproduced with permission.

Social Impact, Responsibility and Media

366 Laura Shin, ChangeTip And Direct Relief Launch Charitable Campaign Using Bitcoin, Forbes (Aug. 19, 2015), http://www.forbes.com/sites/laurashin/2015/08/19/change-tip-and-direct-relief-launch-charitable-campaign-using-bitcoin/.

367 Nikolai Kuznetsov, How Emerging Markets And Blockchain Can Bring An End To Poverty, Forbes (July 24, 2017), https://www.forbes.com/sites/nikolaikuznetsov/2017/07/24/how-emerging-markets-and-blockchain-can-bring-an-end-to-poverty/#515286024a0c.

368 BitGive, About Us (Sept. 21, 2017) https://www.bitgivefoundation.org/about-us/.

369 Paul Vigna and Michael J. Casey, Bitcoin for the Unbanked, Foreign Affairs (Feb. 26, 2015), https://www.foreignaffairs.com/articles/2015-02-26/bitcoin-unbanked.

370 Luis Buenaventura, The Bootstrapper's Guide To Bitcoin Remittances, TechCrunch (Jan. 30, 2015), http://techcrunch.com/2015/01/30/the-bootstrappers-guide-to-bitcoin-remittances/.

371 Bitpesa (last visited Sept. 21, 2017), https://www.bitpesa.co/guide.

372 Coins.ph, (last visited Sept. 21, 2017), https://coins.ph/teller.

373 Digital Citizen Fund, (last visited Sept. 21, 2017), http://www.digitalcitizenfund.org/.

374 Code to Inspire, (last visited Sept. 21, 2017) http://codetoinspire.org/.

375 Carole Vaporean, How learning to code can bring Afghan girls into the global tech marketplace, New York Times (Sept. 07, 2015), http://nytlive.nytimes.com/womeninthe-world/2015/09/07/ceos-afghan-citadel-teaches-women-in-afghanistan-how-to-code/.

376 Andy, WildSpark Beta is Here, Synereo Blog (June 30, 2017), https://blog.synereo.com/2017/06/30/wildspark-beta-is-here/.

377 Robert Hackett, Why Big Business Is Racing to Build Blockchains, Fortune (Aug. 22, 2017), http://fortune.com/2017/08/22/bitcoin-ethereum-blockchain-cryptocurrency/.

378 Jeff John Roberts, Why Celebrities Like Mayweather Could Face Legal Trouble Over ICOs, Fortune (Sept. 11, 2017), http://fortune.com/2017/09/11/ico-bitcoin-celebrities/.

379 Michael del Castillo, Celebrity Investor Mark Cuban is About to Participate in His First ICO, Coindesk (June 29, 2017), https://www.coindesk.com/celebrity-investor-mark-cuban-participate-first-ico/.

380 Michael del Castillo, Who Needs VC? Ethereum and the JOBS Act Could Change Everything, Coindesk (Apr. 10, 2017), https://www.coindesk.com/jobs-act-ethereum-blockchain-capital/.

381 Consumer Financial Protection Bureau, Risks to consumers posed by virtual currencies, (Aug. 2014), http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf.

382 Michael del Castillo, Who Needs VC? Ethereum and the JOBS Act Could Change Everything, Coindesk (Apr. 10, 2017), https://www.coindesk.com/jobs-act-ethereum-blockchain-capital/.

383 Joseph Young, Crowdfunding vs. ICO: Experts Question Legitimacy and Guarantees of Initial Coin Offerings, The Cointelegraph (Oct. 20, 2016), https://cointelegraph.com/news/crowdfunding-vs-ico-experts-question-legitimacy-and-guarantees-of-initial-coin-offerings.

384 Danny Bradbury, Can the Blockchain Save Social Media Influencers?, Nasdaq (June 28, 2017), http://www.nasdaq.com/article/can-the-blockchain-save-social-media-influencers-cm809474

385 "On March 9, 2017, the FTC held its third FinTech Forum, which included presentations and panel discussions on the consumer protection implications of the development of blockchain technologies. Panelists noted that it is difficult to determine the scope of the consumer protection risks posed by blockchain technology because it is in a very early stage of development." Kari S. Larsen and Michael Selig, Federal Trade Commission Considers the Implications of AI and Blockchain Technologies, Reed Smith Client Alerts (Mar. 15, 2017), https://www.reedsmith.com/en/perspectives/2017/03/federal-trade-commission-considers-the-implication.

386 Robert Hackett, Why Big Business Is Racing to Build Blockchains, Fortune (Aug. 22, 2017), http://fortune.com/2017/08/22/bitcoin-ethereum-blockchain-cryptocurrency/.

387 Comcast's Advanced Advertising Group and Participants Announce Blockchain-based Technology Platform, Comcast (June 20, 2017), http://corporate.comcast.com/news-information/news-feed/comcasts-advanced-advertising-group-and-participants-announce-plans-for-blockchain-based-technology-platform-aimed-at-making-premium-video-advertising-more-efficient.

388 MetaX's AdChain product is one example; Shareen Pathak, How blockchain might be useful in marketing and advertising, Digiday (Dec. 15, 2016), https://digiday.com/marketing/blockchain-tech-might-useful-marketing/.

389 Bitteaser (last visited Sept. 21, 2017), https://www.bitteaser.com/.

390 Rebecca Campbell, Babyghost and VeChain: Fashion on the Blockchain, Bitcoin Magazine (Oct. 18, 2016), https://bitcoinmagazine.com/articles/babyghost-and-vechain-fashion-on-the-blockchain-1476807653/.

391 Jeff John Roberts, The Diamond Industry Is Obsessed With the Blockchain, Fortune (Sept. 12, 2017), http://fortune.com/2017/09/12/diamond-blockchain-everledger/.

392 Nexus and Synereo; Steve Olenski, Will Blockchain Reinvent Social Media? Forbes (Aug. 9, 2017), https://www.forbes.com/sites/steveolenski/2017/08/09/will-blockchain-reinvent-social-media/#5b562b383ec1.

393 Steve Olenski, Will Blockchain Reinvent Social Media? Forbes (Aug. 9, 2017), https://www.forbes.com/sites/steveolenski/2017/08/09/will-blockchain-reinvent-social-media/#5b562b383ec1.

394 Jon Berkeley, The Trust Machine, The Economist (Oct. 31, 2015), http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine.

395 Gertrude Chavez-Dreyfuss, Honduras to build land title registry using bitcoin technology, Reuters (May 15, 2015), http://in.reuters.com/article/2015/05/15/usa-honduras-technology-idINKBN0O01V720150515.

396 Id.

397 Id.

398 Jen Wieczner, Why Ethereum is Much More Valuable Than Bitcoin: SoFi CEO, Fortune (July 19, 2017), http://fortune.com/2017/07/19/bitcoin-ethereum-blockchain-sofi/.

399 Shareen Pathak, How blockchain might be useful in marketing and advertising, Digiday (Dec. 15, 2016), https://digiday.com/marketing/blockchain-tech-might-useful-marketing/.

Glossary

400 FinCEN defines "virtual currency" as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction." See Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013), available at https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

Image Credits

p.11 Adapted from loptio: https://github.com/ioptio/design/blob/master/networks/networks.png

p.12 http://spectrum.ieee.org/img/06Bitcoin-1338412974774.jpg

p.85 https://www.coinschedule.com/stats.php

p.86 https://www.coinschedule.com/stats.php

Phone: +44 (0)20 3116 3000
Fax: +44 (0)20 3116 3999
DX 1066 City/DX18 London

ABU DHABI
ATHENS
BEIJING
CENTURY CITY
CHICAGO
DUBAI
FRANKFURT
HONG KONG
HOUSTON
KAZAKHSTAN
LONDON
LOS ANGELES
MIAMI
MUNICH
NEW YORK
PARIS
PHILADELPHIA
PITTSBURGH
PRINCETON
RICHMOND
SAN FRANCISCO
SHANGHAI
SILICON VALLEY
SINGAPORE
TYSONS
WASHINGTON, D.C.
WILMINGTON

reedsmith.com