FinTech

Blockchain

Distributed ledger technology and designing the future

November 2019

Third Edition

ReedSmith

Driving progress through partnership

Contents

Foreword
by the Chamber of Digital Commerce

Once again our good friends at Reed Smith have assembled a comprehensive compendium of U.S. federal and state, as well as non-U.S., laws and developments impacting the blockchain and virtual currency ecosystem. Even one year later, the evolving regulatory climate remains complex and, at times, uncertain. Even more government agencies have claimed jurisdiction over activities using blockchain technology. Recent events and their potential scope globally have prompted regulators worldwide, including central banks, to consider these issues with increased urgency

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 payments, 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, many areas of law continue to remain 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. New digital assets 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.

CHAMBER OF DIGITAL COMMERCE

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

Chapter 1 **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 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." Thereafter, fortune extensively featured the rise of Bitcoin in an 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 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 between bitcoin and Bitcoin 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."

Despite that fact that 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.

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

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

Chapter 2 **Blockchain 101**

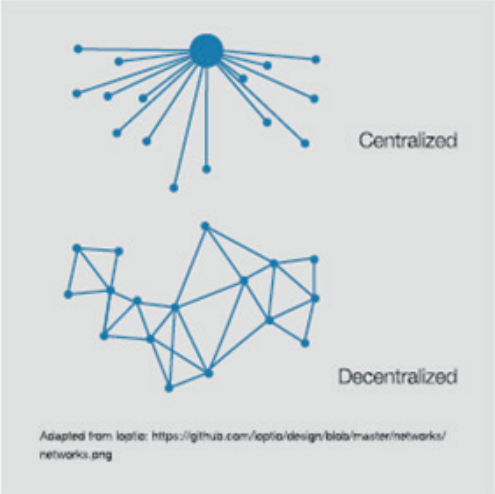
So what is a blockchain? A blockchain is a cryptographically secured database of a continuously growing list of data records that is shared by all parties participating in an established, distributed network of computers. What makes blockchain interesting is that it is a trustless system. That is, blockchain 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. [2]

How it works

A **blockchain**,[3] which is a form of 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 (each, a "node") 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 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 (PoW) consensus algorithm. Participants build new blocks of records by investing computer time (that is, 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 (namely, PoW).



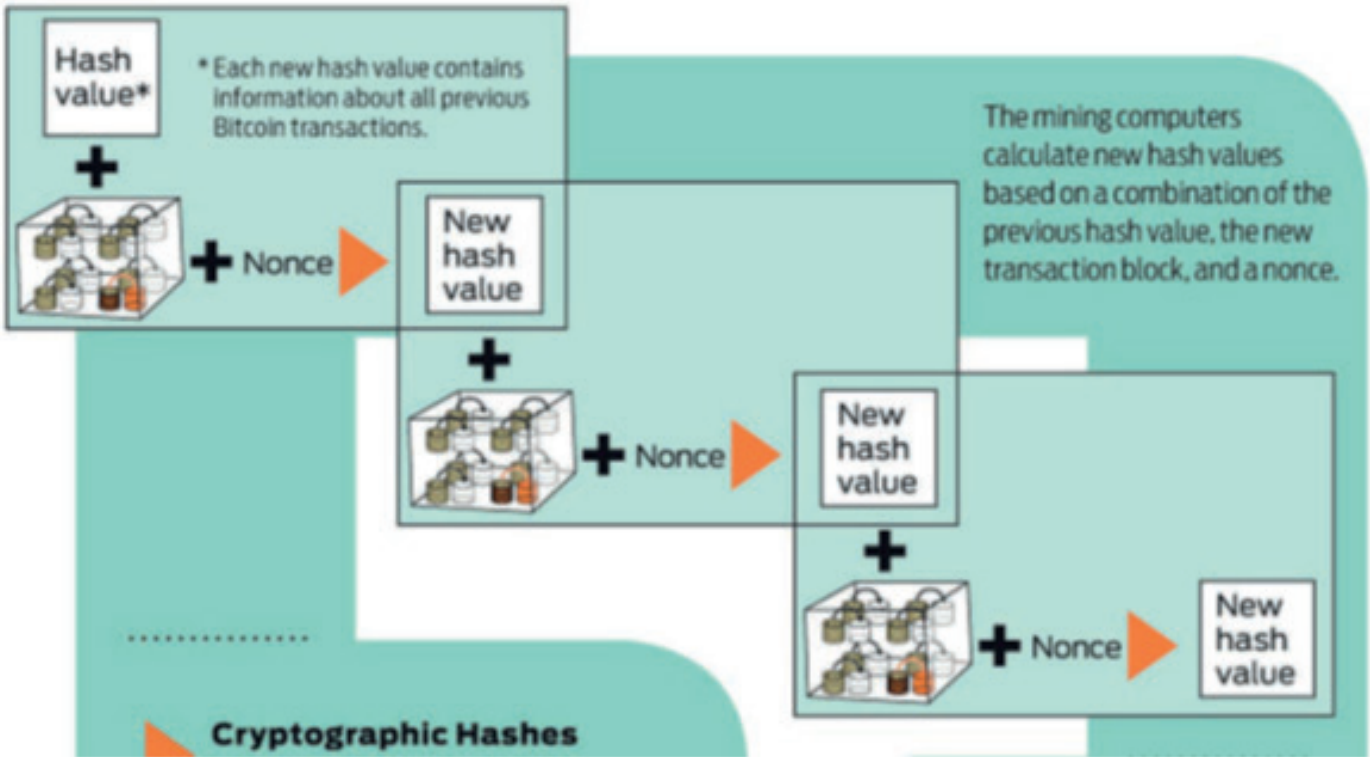
When a user wishes to transfer a digital asset to another user, the user and its counterparty broadcast cryptographically secured digital signatures and the details of their transaction to nearby peers on the network. The users are identified in the transaction by their public keys; this is termed "**pseudonymity**."

When a peer participant solves the mathematical puzzle required to build 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 – they would not only have to re-solve the mathematical puzzle allowing them to create a fraudulent block, but they would also have to re-solve every subsequent block in the blockchain. Even worse for the fraudster, they 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 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.

Despite these built-in accuracy-ensuring qualities, blockchain networks are still vulnerable to certain kinds of cyberattacks. For example, in January 2019, a hacker executed what is known as a "51% attack" on the well-known Ethereum Classic blockchain. In such an attack, a majority of the network's hash rate, or processing power, is concentrated in a single node, thereby allowing that node to manipulate the public ledger at will.[4] With majority control of the network, the attacker was able to create and verify an alternate version of the blockchain on which the attacker could spend funds that had already been spent on the old chain. This type of attack essentially allows a hacker to receiving something for nothing.



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

Digital currencies and "cryptocurrencies"

Digital currencies, which include "cryptocurrencies,"[5] 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.

Although bitcoin was the first cryptocurrency, 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,[6] 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.

Unlike a digital file on your computer, 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 does this system severely reduce the risk of the so-called "double spending" problem, where currency is risked being spent more than once without the involvement of a middleman, but just as importantly, Bitcoin, owing to this middleman elimination, also cuts 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.

Digital currencies, which include "cryptocurrencies," have gained significant attention since the introduction of bitcoin in 2009.

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 by hacking a software client or an exchange 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,[7] 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 trade-offs. Because of latency and scalability issues, many current blockchain applications put severe limits on the size of each new block of 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 on average, 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 can 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.

7

the number of payments per second the Bitcoin network can process

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 PoW 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 their assets on the blockchain forever. For example, as many as 20 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 multifactor 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 new 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 yearlong 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.[8]

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 PoW 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 "51% attacks." 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 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.

20

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

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. For example, since the idea of having one's financial transactions 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.

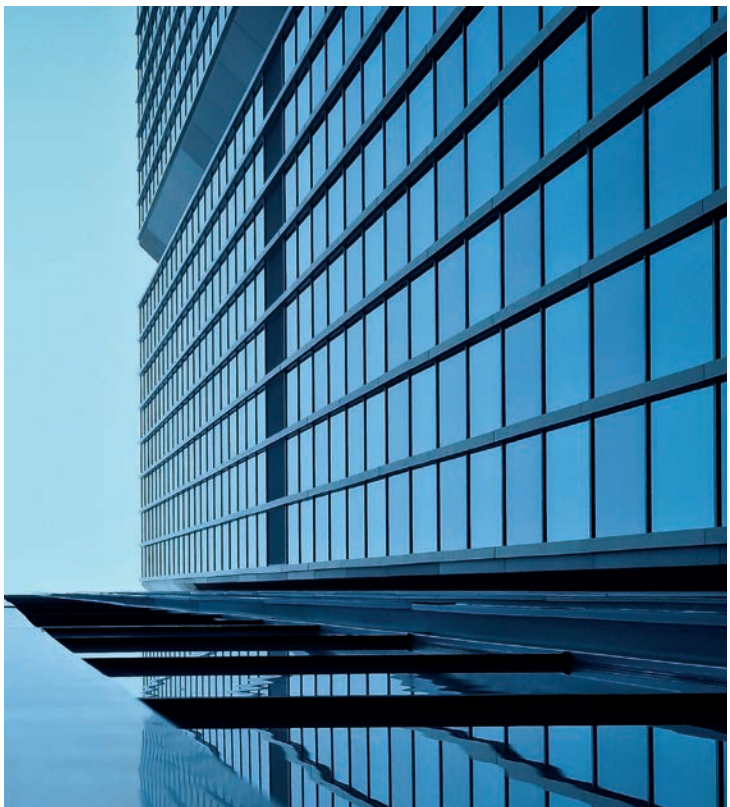
While permissioned blockchains have their obvious security benefits in terms of privacy, predictability, and speed, they are less decentralized, have more single points of failure in the form of fewer permissioned participants, and are less transparent. This has caused critics to view closed distributed 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 are needed to target and infiltrate a closed blockchain, raising important questions about their security.

Proof-of-work vs. proof of stake

One disadvantage of using PoW 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 mathematical puzzle 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 they will obtain a mining fee when new blocks are recorded. This relieves the competitive computing power pressure that causes PoW blockchains to consume excessive energy. Often, proof of stake digital currencies, such as Neo, are treated as a passive investment, wherein the miner's stake gains "dividends" over time.[9] 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 ability of large stakeholders to tamper with the blockchain.

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.

Chapter 3 **Smart contracts**

What are they?

When the Bitcoin blockchain first emerged in 2009, its functionality was quite limited: a user could send bitcoins, or receive them, and nothing more. By 2013, various applications had emerged that used the Bitcoin blockchain as a base structure to conduct more complex transactions, but in the words of Vitalik Buterin, co-founder of Ethereum:

> [They] weren't approaching the problem in the right way. I thought they were going after individual applications; they were trying to kind of explicitly support each [use case] in a sort of Swiss Army knife protocol.[10]

In place of this patchwork system, Buterin imagined a blockchain with a fully integrated programming language capable of performing any instruction that could be coded, no matter how complex. Buterin's blockchain, which launched in 2014 as Ethereum, promised to revolutionize the field of cryptocurrency by expanding its application far beyond financial services, to the entire universe of human activity.

The term "smart contract" can refer either to these coded instructions or to the natural language contracts, which rely on this underlying software for their execution. For clarity, the former can be referred to as "smart contract code" and the latter as a "smart legal contract." The ubiquity of the term can cause confusion, with lawyers more likely to understand smart contracts to be smart legal contracts and programmers more likely to use the term when referring to a piece of code. The two concepts are not distinct, as a smart legal contract will contain smart contract code. It is important to recognize, however, that the existence of smart contract code does not necessarily mean that a smart legal contract exists (as the usual legal requirements of offer, acceptance, consideration and intention to create legal relations must be present).

Smart contract code

Smart contract code works by translating natural language contract terms into their coded equivalent. For instance, consider one term of a traditional contract between a cable television provider and a user: if the user pays their bill, the cable will remain enabled; if they fail to pay, the cable will be turned off. On a blockchain with a fully integrated coding language (also known as a Turing-complete blockchain protocol), this contract term could be translated entirely into code using if/then conditional statements. The product of this translation, a smart contract code, would not require any additional human supervision to accomplish its goal. Whether or not the cable stays on would become a direct function of whether the proper inputs (payment on time) have been met. "Smart" thus refers to the fact that some elements of the contracts are automatic and self-executing in accordance with predefined conditions.

In order to know whether or not the conditions have been met, smart contract code relies on oracles – independent third parties, programs, or agents that control and transmit data onto the blockchain. This outside data, such as pricing information or actuarial tables, allows the smart contract code to have "knowledge" of events in the material world, such as the payment or nonpayment of a cable bill.

Smart contract code can be programmed and run as software on any network. For instance, automatic monthly bill payments are a common example of a smart contract run on a centralized 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 off 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 unless and until Y continues X's cable.

Advantages of smart contracts on blockchains

As alluded to above, smart contract code is already used extensively by centralized networks looking to streamline their operations. When the code is executed on a distributed ledger, however, it changes the playing field substantially. Rather than placing ultimate control over the smart legal contract in the hands of a trusted supervisor, such as the cable company, execution of contract code on a distributed ledger becomes automatic and outside the control of either party. This has the potential to innovatively democratize transactions, granting equal footing and leverage to all parties involved.

Traditionally, contracts – even smart legal contracts – are drafted to be more favorable to the drafter. But the terms of a smart legal contract on the blockchain are immutable and often written entirely in code, substantially reducing their potential for linguistic ambiguity. 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 more likely to fully understand the terms and, consequently, less likely to accidentally breach them.

Although legal issues will still arise in some cases, especially with complex and multilayered smart legal contracts with coded elements as well as natural language ones, transacting through smart legal contracts can potentially lower the incidence and magnitude of these issues.

In addition, by transacting 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 middleman such as a bank or broker to administer the contract's execution. Decreased transaction costs mean that a far higher volume of economic transactions become profitable, including micro-transactions that could form the basis for future decentralized energy grids, water distribution, and smart cities.

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 (see the smart contracts and derivatives section below for more information).

Creative industries can additionally benefit from smart contracts conducted on the blockchain. Because blockchain enables seamless peer-to-peer transactions by buyers and sellers, expensive middlemen such as clearing houses, record companies, and art dealers can be largely removed from the process of exchange. In 2018, a record $317 million art auction was recorded on a distributed ledger meant to track the history and authenticity of all the pieces bought or sold, usurping a role traditionally held by auction houses. [11]

Disadvantages of smart contracts on the blockchain

Though visionaries of the crypto-industry emphasize the bold, sometimes utopian potential for disruption and innovation created by implementing smart legal contracts on the blockchain, there are a few notable disadvantages as well. The most obvious of these is the high initial cost of transferring existing, centralized transactional systems to a new distributed ledger. Existing applications of smart contract technology operating without issue on centralized networks raise the question of whether implementation on a blockchain would be a waste of time, energy, and resources.

Jurisdictional concerns

Another problem with smart contracts is the issue of legal enforceability across multiple jurisdictions. Our existing transactional system, channeled through a few "credible and trusted" global financial actors, took centuries to establish. Although the speed and interconnectivity of the global technological economy means that a new system would not require nearly so much time and energy to institute itself, there will still be substantial lag and turbulence before the enactment of universal standards for interpretation, implementation, and enforcement of smart legal contracts. States and nation states have differing views on the legal standing of electronic signatures, cryptocurrencies (see the regulatory section for a more detailed discussion of this), and blockchain technology as a whole. Many states are still consulting 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 interstate 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.

One final word of caution: despite the proclaimed "smartness" of smart legal contracts, it is worth remembering that they too are products of human minds and are not immune from flaws. As an example, consider the story of the Decentralized Autonomous Organization (DAO), which, being such a key story in the history of DLT to date, is referenced throughout this whitepaper.

The DAO was a highly complex entity composed entirely of smart contract code on the Ethereum blockchain, meant to function as a decentralized hedge fund. Members would contribute money to the DAO, pitch ideas to the community, and vote on which companies or projects deserved funding, all with very minimal human oversight.[12] At the height of the DAO's popularity, in the summer of 2016, the DAO held over $250 million worth of Ether (the currency on the Ethereum network). On June 17, 2016, a still-unknown hacker found a loophole in the code of the DAO that allowed their investment to be withdrawn multiple times over before the balance was changed. Using this exploit, the hacker was able to drain many times the value of their own investment from the network, creating a total loss in excess of $70 million.

In a strictly technical sense (and we do not condone the hacker's actions!), what the hacker did was not theft – it was merely exploiting a loophole in a poorly written smart contract. Just as with contracts written in natural language, minor mistakes in syntax can easily snowball into catastrophic failures. Without the benefit of human oversight, the drafting – and coding – of a smart legal contract takes on even greater importance in the legal process.

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.

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

ISDA's approach

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.

In 2017, ISDA issued a white paper analyzing the possibility of utilizing blockchain technology and smart contract code to realize operational efficiency and cut costs.[13] The white paper distinguishes between operational and nonoperational clauses within the ISDA Master Agreement. On one hand, operational clauses, such as events of default on the occurrence of specified events (see Section 5 of the 2002 Master Agreement) are more suitable to automation and self-execution. These types of clauses would contain conditional logic triggers programmed by smart contract code, which would facilitate the automation of these provisions.

On the other hand, nonoperational clauses that relate to the wider legal relationship between the parties, for example, governing law and disputes clauses (see Section 13 of the 2002 Master Agreement), do not embed conditional logic triggers, making automation more difficult.

In addition, while smart contract code is suited to clauses that trigger obligations, it may not be suited to clauses that trigger rights. For example, clause 6(a) of the 2002 Master Agreement gives the non-defaulting party the right to terminate all outstanding transactions. The white paper notes that the decision to exercise the right is often driven by commercial and relationship factors that are difficult if not impossible to automate. If a smart automatic close-out clause was constructed without regard to these factors, it might be unlawful in the insolvency of one of the parties and deprive the other party of the flexibility needed to manage the market risks arising because of the transactions' termination. This fine balancing act is discussed in great detail in ISDA's second white paper on this topic.

Since 2017 white paper, ISDA has released two further documents, demonstrating its appetite to explore the utility of smart contracts in this field.

In October 2018, ISDA published a white paper entitled "Smart Derivative Contracts: From Concept to Construction."[14] This white paper focuses on the potential transition of smart derivatives contracts from an exciting concept to a universally accepted method of transacting.

In the main, the white paper proposes a five-step practical framework for constructing smart derivatives contracts:

- Selecting parts of a derivatives contract for which automation would be effective and efficient;
- Changing the expression of the legal terms of those parts of the derivatives contract into a more formalized form;
- Breaking the formalized expression into component parts for representation as functions;
- Combining the functions into templates for use with particular derivatives products; and
- Validating the templates as having the same legal effect as the legal terms of a derivatives contract. [15]

The white paper also notes that there are four principles that should be considered in the development of smart derivatives contracts. These are:

1. Compatibility with existing standards;
2. Capability for automation;
3. Effective automation to be based on legal validation; and
4. Benefit of automation

The white paper further explains that smart derivative contracts need to establish and balance technological, commercial, regulatory and legal standards. ISDA's Common Domain Model, which "aims to deliver a standardized model for the post-execution trade lifecycle, focusing on the non-differentiating aspects of that trade lifecycle that are candidates for mutualization by the industry" may provide an effective foundation for this coordination. [16]

The overriding message of the second white paper is that, while the foundations are in place, market proliferation of smart derivatives contracts will only become reality with the coordination of legal, technological, and market expertise. A good example of this is seen in the next ISDA smart derivatives document.

In January 2019, ISDA published a set of introductory legal guidelines for smart derivatives contracts.[17] The guidelines aim to point out certain issues that technology developers may need to consider when developing smart derivatives contracts. The introductory guidelines note that future papers will provide detailed analysis on specific ISDA documents.

In February 2019, ISDA published a second set of legal guidelines, which aims to raise awareness of important legal terms that should be maintained when a technology solution is applied to the ISDA Master Agreement.[18] This set of guidelines breaks the ISDA Master Agreement into five core themes and draws out relevant conditions for technology developers, including but not limited to:

1. Events
   - a Events of default
   - b Termination events
2. Payment and delivery
   - a Suspension of payments
   - b Netting
3. Close-out netting
   - a Early termination
   - b Valuation
4. Disputes
   - a Mechanisms to determine or verify that any data inputs are correct
   - b Remedy of incorrect data inputs
   - c Apportionment for responsibility of errors
5. Contract formation and legal relations
   - a Representations
   - b Transfer of rights
   - c Amendments

The above-mentioned considerations aim to assist developers in addressing the challenges of bringing the benefits of DLT to the life cycle of derivatives transactions, while respecting the legal foundations on which the ISDA architecture is based.

Smart contracts, derivatives, and regulation

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.

Use cases

Some financial institutions are already experimenting with smart contracts and derivatives. Barclays tested R3's Corda platform to execute swaps using smart contracts as early as 2016.[19] DTCC and six other firms similarly tested blockchain technology that uses smart contracts to manage post-trade life cycle events for credit default swaps.[20] We expect to see more smart contract implementation in financial markets in the near future. Additionally, in a white paper published in April 2018,[21] the Commodity Futures Trading Commission (CFTC) discussed DLT as having significant potential for handling swap data, explaining that DLT could allow the CFTC and other regulators to access swaps data automatically and seamlessly from reporting counterparties every time a swap is executed or updated on a particular blockchain, without the need for human intervention or the use of other intermediaries. The CFTC recognized that adopting such technology would increase the speed in which regulators could access data and could also increase the reliability of the data while reducing the costs of making the data available to regulators. The CFTC further made recommendations regarding interoperability of systems, long-term technology strategy, and security for regulators to follow as firms adopt DLT utilities. [22]

Smart contracts – going forward

The possibilities for broader acceptance and enforceability of smart contracts continues to be discussed. For example, in May 2019, the UK Jurisdictional Taskforce (UKJT) published a consultation paper requesting submissions from stakeholders working with, or interested in, crypto assets, DLT, and smart contracts.[23] As part of the consultation process, the UKJT is interested in determining the enforceability of smart contracts and the circumstances under which a smart contract is capable of giving rise to binding legal obligations. The consultation paper highlights the need to clarify how the general principles of contractual interpretation by a court may need to be recalibrated when applied to smart contracts. There are also concerns over how parties may be able to enforce their rights and rely on smart contracts in the event that the technology malfunctions or does not perform as expected

Chapter 4 **Applications of DLT**

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 developed a financial grade open source distributed ledger platform known as Corda. Delaware passed legislation that allows Delaware chartered companies to maintain their stock ledgers via DLT.[24] Arizona passed a law clarifying that so called "smart contracts" made in computer code on a blockchain are enforceable.[25] The California Assembly and Senate passed a bill amending the Uniform Electronic Transactions Act to add a definition of blockchain as "a mathematically secured, chronological, and decentralized ledger or database," and to require the Government Operations Agency of the Department of General Services to appoint a working group to evaluate the use of blockchain in state government and businesses in California by July 1, 2019. Other states including Tennessee and Wyoming have proposed or enacted legislation to recognize the legal authority to use blockchain technology to conduct transactions or to record and store corporate records.[26] 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. [27]

The blockchain has also garnered attention from government agencies and regulators. For example, the U.S. Office of the Comptroller of the Currency (OCC) has implemented a framework where FinTech companies can 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.

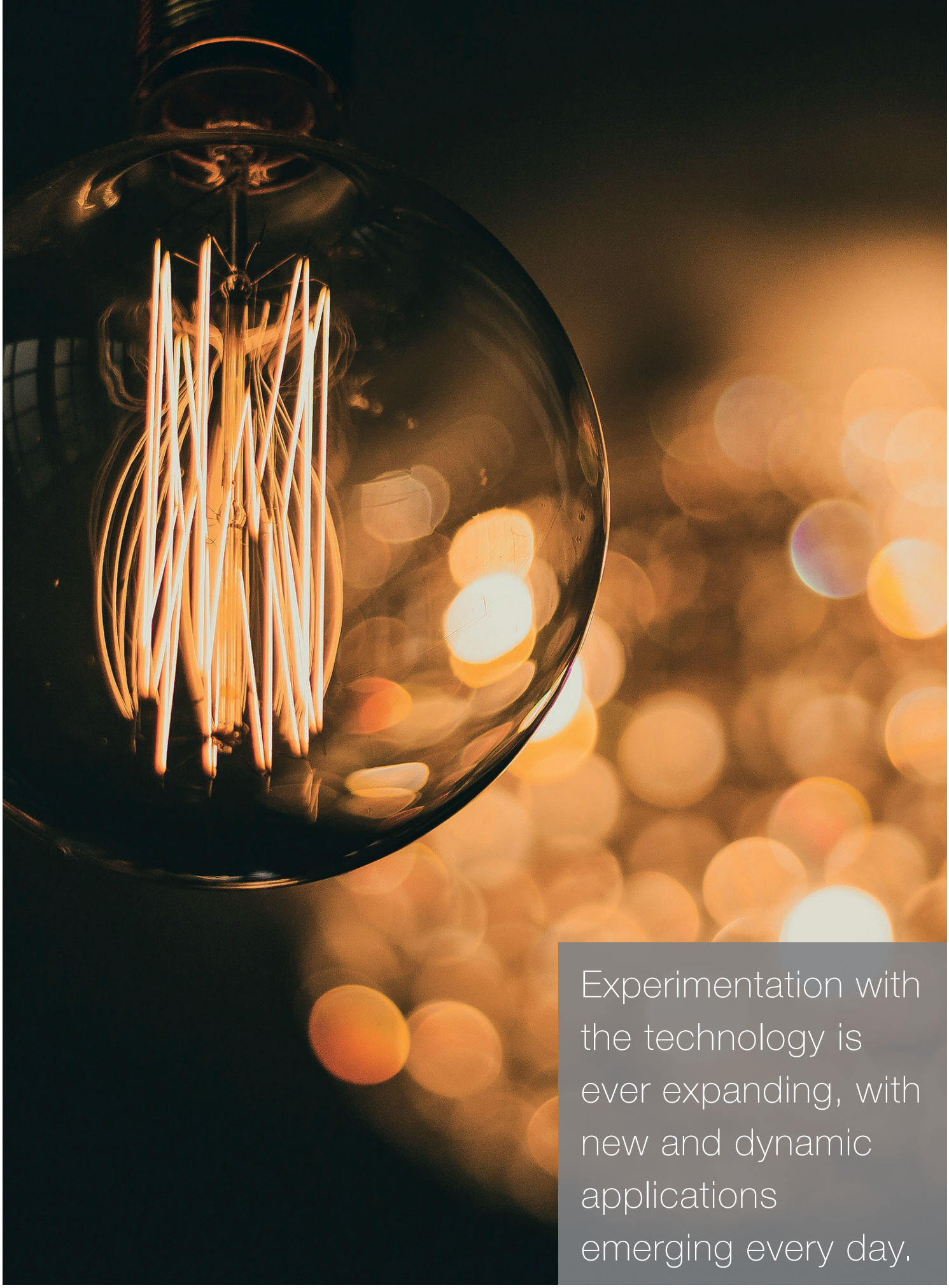
The application of the blockchain is anticipated to extend far beyond financial services to include various applications of authentication, supply chain management, data storage, real property records, digital content ownership verification, and business process management. Experimentation with the technology is ever expanding, with new and dynamic applications emerging every day.

Tokens

The first practical application of blockchain technology was bitcoin. As discussed earlier in this whitepaper, it was originally developed to facilitate online payments without the need for a "trustworthy third party" – usually a financial services provider – to act as an intermediary.

Since 2015, Initial Coin Offerings (ICOs) have emerged as a new, DLT-based form of financing. ICOs commonly involve the issuance of "cryptotokens" or "cryptoassets", which are a digital, cryptography- and DLT-based representation of an intrinsic or perceived value. This value can be based on a wide range of functionalities, properties or rights associated with the token.

Many of the regulatory developments in the recent history of blockchain and DLT relate to the regulatory treatment of these tokens. This is discussed in the detail in the next two chapters.



Experimentation with the technology is ever expanding, with new and dynamic applications emerging every day.

Chapter 5 **U.S. regulatory landscape**

In the United States, it is currently legal to transmit, mine, and develop "virtual currencies,"[28] 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 DLT for both monetary and nonmonetary 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 (and related enforcement) 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 OCC 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 DLT for nonmonetary purposes from the states' respective money transmission statutes.

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

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.[29] 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."[30]

As of July 2018, NYDFS had approved 10 firms for virtual currency charters or licenses, granted licenses to bitFlyer USA, Circle Internet Financial, Coinbase Inc., Genesis Global Trading Inc., Square, Inc., Xapo, Inc., and XRP II, and granted charters to Gemini Trust Company and Paxos (formerly itBit Trust Company). As of October 2017, NYDFS had denied five BitLicense applications and ordered the companies receiving denial letters to stop any operations in New York. [31]

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. [32]

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.[33] 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. [34]

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 [35]

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

BitLicense exempts several activities from licensure. For example, virtual currency mining on its own would not subject a party to the BitLicense regime.[36] Similarly, consumers or merchants only using virtual currency to buy or sell goods or services would not be required to obtain a license.[37] And finally, parties who engage purely in software development and dissemination do not fall under BitLicense.[38] 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."[39] 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.

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

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.[40] Under BitLicense, NYDFS must approve or deny applications within 90 days of deeming the application complete.[41] 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.[42] Therefore, as with the licensing processes 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.[43] 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.

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.[44] 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. [45]

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.[46] This policy is subject to both an initial risk assessment and ongoing annual risk assessments.[47] 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.[48] The policy must be subject to annual independent testing, and the audit report must be submitted to NYDFS. [49]

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.[50] Licensees must identify and verify customers' identities, check customers against the list of Specifically Designated Nationals maintained by the Office of Foreign Assets Control, and ma intain customer records.[51] 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. [52]

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

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

- Capital requirements [53]
- Custody and protection of assets [54]
- Books and records [55]
- Consumer protection disclosures [56]
- Consumer complaint policies [57]
- Advertising[58] anti-fraud policies [59]
- Cybersecurity programs [60]
- Business continuity and disaster recovery plans [61]

Under BitLicense, licensees are subject to at least one examination by NYDFS every two years.[62] Licensees must also submit numerous financial statements and reports to NYDFS on a quarterly and annual basis. [63]

Additionally, New York's virtual currency laws require a digital currency transmitter that engages in the business of selling or issuing checks, receiving money for transmission or transmitting money to obtain a money transmitter license, and thus certain companies may be required to obtain BitLicenses as well as a New York money transmitter license.

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.

California

In June 2015, the California House of Representatives passed AB-1326.[64] The bill, introduced in February 2015, would provide for a similar, but not quite as extensive, licensing regime to New York's BitLicense.[65] 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.[66] The bill is no longer listed as active; however, it could be revived on a future date.

Connecticut

On June 19, 2015, shortly after enactment of New York's BitLicense regime, Connecticut Governor 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. [67]

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." [68]

New Hampshire

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.[69] The definition of "monetary value" was amended to specifically include "convertible virtual currency." [70]

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." [71]

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." [72]

North Carolina

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." [73]

The Act also specifically defines "money transmission" to include "maintaining control of virtual currency on behalf of others." [74] 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. [75] 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." [76]

Washington

In April 2017, the state of Washington signed Senate Bill 5031, placing all operators of virtual currency under the jurisdiction of Washington's money transmitter laws. [77] 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.

Other state regulation

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.[78] However, Wyoming, New Hampshire, 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 six 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.[79] The guidance from the Illinois Department of Financial and Professional Regulation also explicitly provides that virtual currency mining, use or development of multi-signature software, and use of a virtual currency's blockchain or DLT for nonmonetary purposes (including smart property and smart contracts) would not be considered money transmission under the Illinois Transmitters of Money Act. [80]

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. [81] Perhaps more significantly, the department also informed Coinbase that virtual currency would not be considered a "permissible investment" under the statute. [82] 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. [83]

The practical effect of the Hawaii 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. [84] 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."

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." [86] 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. [87]

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.[88] 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." [89]

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. [90]

Conference of State Bank Supervisors

On September 15, 2015, the Conference of State Bank Supervisors (CSBS) 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 (for example, wallets, vaults, kiosks, merchant-acquirers, and payment processors)" be supervised and licensed by state banking regulators. [91] "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. [92]

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. [93] 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 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. [94] 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. [95] In 2018, Arizona introduced Bill 2601, which excludes "virtual coin," defined as a "digital representation of value that can be digitally traded and that functions as a medium of exchange, unit of account and store of value," from state securities laws. [96]

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." [97] In July 2018, Vermont's SB 269, Act 205, An Act Relating to Blockchain Business Development, went into effect creating the Blockchain-Based Limited Liability Company and the Personal Information Protection Company as new types of entities under Vermont Law. The Blockchain-Based Limited Liability Company (BBLLC) is a limited liability company organized for the purpose of operating a business that utilizes blockchain technology for a material portion of its business activities, which elects to become a BBLLC. The act authorizes a BBLLC to use blockchain technology for its governance, in whole or in part, and to adopt any reasonable algorithmic means for accomplishing the consensus process for validating records, as well as requirements, processes, and procedures for conducting operations, or making organizational decisions on the blockchain technology used by the BBLLC. The Personal Information Protection Company is a business organized for the primary purpose of receiving, holding, and managing the

disclosure or use of personal information for individual customers. A Personal Information Protection Company has a fiduciary relationship to the customer and is required to first obtain a certificate of authority from the state.

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.[98] 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, and financial markets. [99]

In March 2018, Governor Matt Mead of Wyoming signed into law multiple blockchain-related bills. HB0019 provides an exemption from the Wyoming Money Transmitter Act for anyone who buys, sells, issues, or takes custody of virtual currency or who receives virtual currency for transmission. [100] HB0070 exempts from state securities law a developer or seller of an open blockchain, provided certain conditions are met. [101] HB0101 permits Wyoming corporations to use blockchain for record keeping purposes. [102] SF0111 exempts virtual currencies from property taxation. [103]

In August 2018, Ohio passed Senate Bill 220, clarifying the legal status of records, contracts, and signatures secured through blockchain technology by adding them to the definitions of "electronic record" and "electronic signature."

On September 20, 2018, the Division of Banking of Colorado's Department of Regulatory Agencies issued an Interim Regulatory Guidance, which declared that cryptocurrencies are not recognized as legal tender or fiat currency, the direct transmission of cryptocurrency between two consumers is not subject to money transmitter licensure, and, in transactions that involve a third party, the transmission solely of cryptocurrency between one consumer and another is not money transmission. Cryptocurrency exchanges that do handle fiat currency may be subject to money transmitter licensure and requirements. [104]

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.

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. [105] Under the CEA and its regulations, the CFTC has jurisdiction over the trading of futures, options, and swaps on "commodities." [106] The term "commodity" is defined broadly to include "goods and articles...and all services, rights and interests..." [107] 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.[108] 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. [109] Further, as described in detail below, on September 26, 2018, a federal district court judge in Massachusetts upheld the CFTC's jurisdiction over virtual currencies, broadening the Commission's jurisdiction to include all virtual currencies, even those that are not the subject of an underlying futures contract. 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 (NFA).

Self-regulators such as the Financial Industry Regulatory Authority (FINRA) and the NFA began questioning its member companies about their dealing in cryptocurrency as recently as December 2017 when the CFTC issued a notice to its members requiring each entity to notify the organization if it engages or plans to engage in virtual currency transactions. Even more recently, in July 2018, the NFA issued a letter to its members with a proposed interpretive notice on requirements for disclosures to customers on the risks associated with virtual currency and trading. 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 and a swap execution facility under the CEA. [110] 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. [111]

The CFTC launched LabCFTC, a fintech initiative that seeks to foster responsible innovation, in 2017. [112] LabCFTC works with fintech companies to assist them in understanding how the U.S. commodities laws and regulations might affect their business. On February 19, 2018, the CFTC and UK's Financial Conduct Authority (FCA) announced that they had entered into an arrangement that commits both parties to collaborate and support innovative firms through the CFTC's LabCFTC and the FCA's counterpart, FCA Innovate. [113] The Cooperation Arrangement on Financial Technology Innovation, which represents LabCFTC's first arrangement with a non-U.S. counterpart, focuses on information-sharing regarding fintech market trends and developments and "facilitates referrals of fintech companies interested in entering the others' market, and sharing information and insight derived from each authority's relevant sandbox, POC, or innovation competitions." [114]

Financial Crimes Enforcement Network (FinCEN)

Like the CFTC, FinCEN has not issued any final regulations directly addressing virtual currency. However, FinCEN has asserted its authority to regulate virtual currency pursuant to its mandate under the Bank Secrecy Act (BSA) to police money laundering. In March 2013, FinCEN issued guidance asserting that businesses that (i) "exchange... virtual currency for real currency, funds, or other virtual currency;" or (ii) issue virtual currency and have the authority to withdraw it from circulation constitute money transmitters under the BSA and therefore are subject to FinCEN's registration, reporting, and recordkeeping requirements, including know your customer compliance requirements and the requirement to establish AML programs.

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." [115] However, in February 2018, in a letter from the Department of the Treasury Office of Legislative Affairs, FinCEN stated that generally, under existing regulations and interpretations, a developer that sells convertible virtual currency, including in the form of initial coin offerings (ICO) coins or tokens, in exchange for another type of value that substitutes for

currency is a money transmitter and must comply with AML/CFT requirements that apply to this type of MSB.

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." [116] 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.

Money transmitters must comply with the BSA and its implementing regulations. Complying with the BSA includes "registering with FinCEN as a MSB; preparing a written AML compliance program that is designed to mitigate risks (including money laundering risks) associated with the entity's specific business and customer mix, and to ensure compliance with other BSA requirements; filing BSA reports, including suspicious activity and currency transaction reports; keeping records for certain types of transactions at specific thresholds; and obtaining customer identification information sufficient to comply with the AML Program and recordkeeping requirements." [117]

It is a federal crime to knowingly conduct an MSB while failing to register with FinCEN (or state licensing money transmission licensing agencies). [118]

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). [119]
- 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. [120]

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; [121]
- Use of virtual currency to purchase goods and services; [122]
- Conversion of virtual currency to fiat currency for one's own use; [123]
- Investing in virtual currency for one's own account; [124]
- Renting out of computer systems and software that mine virtual currency to third parties (where any virtual currency mined by the third party using the software would remain the property of that third party); [125]
- 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; [126]
- Maintaining a set of book accounts where customers may deposit virtual currency; [127]
- 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; [128]
- 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. [129]

Citing guidance issued in 2014, in February 2018, Drew Maloney, Assistant Secretary for Legislative Affairs for FinCEN, indicated that "a developer that sells convertible virtual currency, including in the form of ICO coins or tokens, in exchange for another type of value that substitutes for currency, is a money transmitter and must comply with AML/CFT requirements" applicable to that type of MSB. [130] However, he further indicated that the structure of such ICOs would determine whether its requirements would apply to such ICO or that of another regulator. [131]

On September 12, 2018, the U.S. House of Representatives voted to strengthen the power of FinCEN to fulfill its duty to, among other things, protect the U.S. financial system from illicit use, money laundering, and terrorism. Under the FinCEN Improvement Act of 2018, the House included tribal law enforcement officials within the agencies FinCEN is charged with coordinating with and clarified that "anti-terrorism and AML "initiatives" included "matters involving emerging technologies or value that substitutes for currency, and similar efforts." [132] On September 17, 2018, the bill was referred to the Senate Banking, Housing and Urban Affairs Committee.

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

Office of the Comptroller of the Currency

In December 2016, the OCC announced it would consider granting fintech firms special purpose national bank charters.[133] In September 2018, the OCC announced that it would begin accepting such special purpose bank charters. The charter standards for processing fintech applications will be the same as those currently outlined in the Comptroller's Licensing Manual. Consistent with its treatment of all national banks, "the OCC will consider whether a proposed bank has a reasonable chance of success, will be operated in a safe and sound manner, will provide fair access to financial services, will treat customers fairly, and will comply with applicable laws and regulations." [134] Although fintech companies receiving national bank charters will be subject to the same high standards as other federally chartered banks, the OCC will take into account "the bank's size, complexity, and risk profile, consistent with applicable law." [135]

In order to apply for a special purpose national bank charter, a fintech company must be in the "business of banking, which includes receiving deposits, paying checks, or lending money."[136] 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." [137]

Fintech firms receiving a special purpose national bank charter are subject to the "OCC's regulatory scrutiny, and the OCC has previously indicated it would hold such companies to rigorous standards on issues concerning safety and soundness, capital requirements, AML," financial inclusion and consumer protection.[138] Although the regulatory and compliance burdens for fintech firms with a special purpose national bank charter will be high, the fintech companies receiving such charters will benefit from only having to follow a single, uniform set of regulations as opposed to 50 sets of state regulations that may be inconsistent and difficult to track.

The idea of special purchase national bank charters for fintech companies has generally been greeted positively by fintech firms that have argued that the current U.S. regulatory structure hurts innovation, and that the special purpose national bank charters for fintech companies will reduce regulatory complexity and allow companies to more easily operate nationwide. [139] This is 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 the best to 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." [140] On April 26, 2017, 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. [141] 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. [142]

Both cases, which were filed prior to the OCC issuing the policy statement that it would allow fintech firms to apply for special purpose bank charters, were subsequently dismissed on the grounds that they were not ripe for review by the court. [143] Now that allowing fintech firms to receive federal charters is the "OCC's official policy," New York has again filed suit against the OCC, seeking a declaration that the OCC exceeded its authority under the National Bank Act and violated the Constitution's 10th Amendment by usurping state powers. To date, no company has filed for charter approval as a new special purpose bank.

Securities and Exchange Commission

As the use of digital assets and virtual currency exchanges have become more prominent, the SEC has taken a more aggressive position on its power to regulate transactions involving those assets and structures. ICOs have been of particular interest to the SEC.

On July 25, 2017, the SEC issued an Investigative Report detailing its investigation of an ICO of crypto tokens representing interests in the DAO through the Ethereum blockchain. 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 placed this subset of crypto assets within the catchall category of securities known as "investment contracts" and stated that it would use the facts and circumstances test set forth in the 1946 U.S. Supreme Court decision in SEC v. Howey to determine whether a given product must be offered in conformity with the federal securities laws. Several federal courts have since confirmed that the Howey analysis is the appropriate vehicle for determining whether a particular digital token constitutes a security. [144] Since the SEC issued the Investigative Report, SEC Chairman Jay Clayton has taken the affirmative stance that ICOs represent offerings of securities and has confirmed that the analysis applied in the Investigative Report remains relevant despite the changing regulatory landscape. [145]

On February 6, 2018, Chairman Clayton said during a U.S. Senate hearing that "by and large, the structures of ICOs that [he has] seen involve the offer and sale of securities and directly implicate the securities registration requirements and other investor protection provisions" of federal securities laws. [146] He also reiterated the SEC's long-standing position that the structure and branding of a product would not necessarily stop the SEC from exercising its authority to regulate. Specifically, he noted that some ICOs, despite having "utility or voucher-like characteristics," would fall under federal securities laws and that styling the underlying digital asset as a "utility token" would not prevent the SEC from using its regulatory authority. [147] As William Hinman, the Director of the SEC's Division of Corporation Finance, pointed out when comparing the oranges sold in Howey to utility tokens, the defense in Howey failed in its argument that the defendant was selling oranges for consumption, and those arguing that coins labeled "utility coins" take ICOs out of the purview of SEC regulators will similarly fail, even in instances where the coins have some utility. [148]

In April 2019, the SEC's Strategic Hub for Innovation and Financial Technology (FinHub) provided much needed clarity in the SEC's position on digital assets when it published the "Framework for 'Investment Contract' Analysis of Digital Assets" (Framework), memorializing much of Director Hinman and Chairman Clayton's commentary. In a public statement announcing its release, the SEC billed the Framework as an "analytical tool to help market participants assess whether the federal securities laws apply to the offer, sale, or resale of a particular digital asset." [149] The Framework, which discusses how different characteristics of digital assets and ICOs influence the Howey analysis, provides the most comprehensive analytical structure for assessing digital assets to date.

The Framework authors cite, as an example, a hypothetical token issued by a fully developed online retailer that sells a non-transferrable digital asset to its customers for use in its network. Where the token can only be used, and can be immediately used, to purchase products from the retailer, the Framework concludes, "the digital asset would not be an investment contract." [150]

Also in April 2019, the SEC's Division of Corporation Finance issued a response to a no-action request submitted by TurnKey Jet, Inc., (TurnKey), a provider of air charter services. [151] In the first SEC no-action letter addressing a blockchain-based project, the SEC indicated it would not pursue an enforcement action if TurnKey sold a digital token (TKJ) to its air charter customers, under the circumstances outlined in TurnKey's letter. In its brief response, the SEC identified several factors as particularly important to its conclusion that TurnKey need not register TKJ as a security, including that the TurnKey platform will be fully developed and operational before and independent of any token sales, TKJ will not be transferrable outside of the TurnKey ecosystem, and TKJ will be pegged to a value of one USD per token and represent the right to receive services worth one USD.[152]

Between the Framework and the TurnKey no-action letter, the SEC appears to be staking out the boundaries of a safe-harbor for digital assets that are non-transferrable, immediately usable, lack other speculative qualities, and are issued in connection with a fully developed platform. These pronouncements are consistent with and continue a seemingly deliberate path by the SEC providing guidance to the industry.

Chairman Clayton recently reiterated that the SEC regulates "securities transactions and certain individuals and firms who participate in our securities market" and that it did "not have direct oversight of transactions in currencies or commodities, including currency trading platforms." [153] On April 12, 2018, Chairman Clayton described a regulatory continuum, with cryptocurrency like bitcoin on one side and tokenized securities offered as part of an ICO on the other. According to Chairman Clayton, SEC jurisdiction lies on the tokenized securities end of the continuum. He noted that some tokens can begin as securities and, over time, become non-securities and vice versa, depending on the economics of the token, [154] a view that he recently reaffirmed.[155]

Chairman Clayton's evolving stance represented a point of confusion in the industry, as the SEC's inquiry into whether Ethereum was a security fomented uncertainty and a drag on the cryptocurrency market until June 2018, when the SEC determined that Ethereum is not a security. [156] On June 6, 2018, Chairman Clayton further clarified that bitcoin is not a security. [157]

On May 2, 2018, SEC Commissioner Hester Peirce stated at an industry conference that she was "wary of any blanket designation for all ICOs." Going further, she noted that regulators should "evaluate the facts and circumstances of each offering." [158] In May 2018, SEC Commissioner Robert Jackson expressed an intent to bring ICOs in line with SEC rules and regulations; however, he noted that the SEC's current focus is on protecting investors from fraud. [159]

Although the SEC's stance on cryptocurrency and ICOs continues to evolve, its concern with fraud has been a continuing theme. In March 2017, the SEC rejected two separate bids to list bitcoin-backed ETFs, which would only hold bitcoin as assets. One of those bids, an application for the Winklevoss Bitcoin Trust, sought to be listed on the Bats BZX Exchange – one of the largest ETF exchanges. [160] 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." [161] 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." [162] 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." [163] Yet 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." [164] 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. [165] The SEC went on to review its decision to reject the Winklevoss Bitcoin Trust, but eventually affirmed that decision in July 2018. [166]

In September 2017, the SEC 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. [167] One area of the Cyber Unit's stated focus will be potential violations involving distributed ledger technology ICOs. It is likely that the SEC will continue to aggressively pursue those involved in ICOs when they fail to abide by federal securities laws.

On December 4, 2017, NYSE Arca, Inc. (NYSE Arca) proposed a rule change in order to list and trade shares of ProShares Bitcoin ETF and ProShares Short Bitcoin ETF issued by ProShares Trust II. After allowing for comments and considering the proposed rule change, the SEC disapproved the rule change on August 22, 2018. [168] Summarizing its principal concerns, the SEC indicated that NYSE Arca did not meet its burden under the Securities Exchange Act of 1934 (Exchange Act) and the SEC's Rules of Practice "to demonstrate that its proposal is consistent with the requirements of the Exchange Act Section 6(b)(5), in particular the requirement that a national exchange's rules be designed to prevent fraudulent and manipulative acts and practices." [169] On September 20, 2018, the SEC announced that it was seeking additional comments on a proposed rule change to list and trade shares of SolidX Bitcoin Shares, issued by the VanEck SolidX Bitcoin Trust, with BZX Exchange, Inc. [170] As of August 2019, the SEC still had not made a determination with regards to the VanEck SolidX Bitcoin Trust.

Shortly after issuing the DAO Investigative 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. [171] On August 23, 2017, the SEC issued an order suspending trading in the securities of First Bitcoin Capital Corp., a Canadian company that had 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. [172] 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 intended 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. [173]

The SEC's decisions have not been without consequence. For example, on March 3, 2017, prior to the SEC's decision in the Winklevoss case discussed above, when many investors anticipated a favorable outcome, the price of bitcoin hit a record high; following the rejection on March 10, the price fell by 18 percent; and following the SEC's decision to reconsider its rejection, bitcoin rebounded to hit another near high. [174]

In January 2018, Chairman Clayton and CFTC Chairman J. Christopher Giancarlo stated their intent to "continue to work together to bring transparency and integrity to these markets and, importantly, to deter and prosecute fraud and abuse." [175] In its efforts to prevent and punish fraud related to ICOs and cryptocurrency, the SEC has halted ICOs, rejected cryptocurrency ETFs, and continues to initiate a growing number of enforcement actions.[176] The SEC was also reported to have issued 80 subpoenas to digital asset companies as of March 2018, [177] some of which have materialized into new enforcement actions. [178] These efforts will likely continue throughout 2019 and beyond. (Please refer to the enforcement section below for more detail on SEC enforcement actions.)

In October 2018, the SEC announced the launch of the agency's FinHub, which will serve as a resource for public engagement on the SEC's fintech-related issues and initiatives, including digital assets. [179] As part of its services for industry professionals, FinHub held the first Fintech Forum on May 31, 2019, where industry professionals and regulators held a panel discussions on topics including investment management, capital formation, trading and markets, and innovations in DLT. [180]

The SEC has not limited its scrutiny to fraudulent projects, and in November 2018 announced two settlements, one with CarrierEQ Inc. (AirFox) and the other with Paragon Coin Inc., marking the first time that the SEC has imposed civil penalties on companies solely for offering digital tokens in an ICO that allegedly violates the

securities laws absent any allegations of fraudulent statements. [181] Reflecting the SEC's stated view that there are compliant ways to market for digital asset issuers, AirFox and Paragon agreed to pay penalties and to register the tokens they sold as securities under Section 12(g) of the Exchange Act. [182]

The SEC also continues to encourage market participants to work cooperatively with the Commission to find ways to conduct a compliant-ICO. In addition to the TurnKey Jet no-action letter mentioned above, on February 20, 2019, the SEC accepted a settlement offer from a blockchain company, Gladius Network LLC, which self-reported its ICO to the SEC. [183] In turn, the SEC did not penalize Gladius, which agreed to offer customer refunds and to register its tokens as securities.

Other market participants are also pursuing compliant-ICOs utilizing existing regulatory frameworks. For example, in April 2019, Blockstack Token LLC filed a preliminary offering circular with the SEC for a $50 million Regulation A offering. [184] The offering was later approved by the SEC. Reflecting the SEC's position the whether a token is a security can change over time depending on the circumstances, Blockstack's offering expressly stated that it anticipates its tokens may not be treated as securities in the future.

Internal Revenue Service (IRS)

The IRS has concluded that digital currency should be considered "property" under the Internal Revenue Code, and thus transfers involving virtual currencies would be taxable events. [185] 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." [186] Perhaps not coincidentally, the IRS appears to have become more aggressive recently in attempting to enforce potential tax violations involving virtual currency transactions. For example, 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. [187] Under federal law, the

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

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." [188] Calls for clarity continue nonetheless. On May 30, 2018, the American Institute of CPAs (AICPA) released a letter calling for additional guidance on the tax treatment of virtual currency transactions. [189] Although the IRS released Notice 2014-21, AICPA requested that the IRS address the topics in its guidance with greater specificity and that it address new issues not previously included in its guidance. [190]

Financial Industry Regulatory Authority

In January 2017, FINRA issued a detailed report entitled 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 DLT 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. [191]

On July 6, 2018, FINRA issued Regulatory Notice 18-20 "to encourage each firm to promptly notify FINRA if it, or its associated persons or affiliates, currently engages, or intends to engage, in any activities related to digital assets, such as cryptocurrencies and other virtual coins and tokens." [192] FINRA also requested that, until July 31, 2019, each firm "keep its Regulatory Coordinator abreast of changes in the event the firm, or its associated persons or affiliates, determines to engage in activities relating to digital assets not previously disclosed." [193]

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, the Federal Deposit Insurance Corporation, and the North American Securities Administrators Association. Notably, however, while the CFPB has issued a consumer advisory regarding digital currency, [194] the agency explicitly declined to include regulation of digital currency as part of its recent Prepaid Rule. [195] On September 13, 2018, the CFPB proposed the creation of a Disclosure Sandbox disclosure program for covered persons to be in compliance with or exempt from a requirement of a CFPB rule or certain federal laws. [196] On August 7, 2018, the CFPB announced that it had joined the Global Financial Innovation Network (GFIN), a group of 11 financial regulators and related organizations seeking to promote innovation and efficient regulation, in addition to creating a framework for cooperation between financial services regulators.[197]

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. [198]

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. [199]

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. [200] 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.

On August 23, 2018, the CFTC won a trial against Patrick K. McDonnell and CabbageTech, Corp., doing business as CDM. CDM was alleged to have provided real-time expert virtual currency trading advice and conducted virtual currency purchasing and trading on behalf of its customers in exchange for money and virtual currencies. According to the CFTC, CDM

engaged in a deceptive and fraudulent scheme whereby CDM, under McDonnell's direction, misappropriated customer funds. In a prior complaint filed under this action, the court found that the CFTC's anti-fraud authority applies to the use or attempted use of any manipulative or deceptive device in connection with a contract or sale of any commodity in interstate commerce, which included the virtual currencies at issue. Defendants McDonnell and CDM were ordered to pay over $1.1 million in penalties and restitution. [201]

On September 26, 2018, a U.S. federal judge decided that the CFTC had jurisdiction in its case against My Big Coin Pay Inc. because virtual currency meets the definition of a commodity. The decision marks a turning point in CFTC enforcement actions. According to the court, while there did not exist a futures market for My Big Coin Pay Inc., the virtual currency at issue, the existence of futures trading within the general class of virtual currency was sufficient to designate virtual currency as a commodity and subject to the jurisdiction of the CFTC. [202]

FinCEN

On May 15, 2015, FinCEN issued a $700,000 civil monetary penalty against Ripple Labs, Inc. for willful violations of the BSA 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. [203]

On July 27, 2017, FinCEN fined BTC-e, a virtual currency exchange, $110 million for facilitating transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking. [204]

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 held, that Bitcoin Savings & Trust and Shavers conducted a Ponzi scheme soliciting investments in bitcoin-related investment opportunities.[205]

In December 2014, the SEC sanctioned Ethan Burnside for operating two digital currency exchanges without registering them as either broker-dealers or stock exchanges. [206]

In June 2014, Erik Voorhees 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. [207]

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 investment proceeds from newer investors. [208]

In July 2016, the SEC settled charges against Bitcoin Investment Trust and SecondMarket, Inc., alleging that the two entities violated Regulation M. [209] 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. [210] 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 sizable returns from the companies' operations, when the companies had no real operations. On October 27, 2017 the DOJ brought its own proceeding against Zaslavskiy for securities fraud in connection with the same pair of ICOs, and on September 11, 2018, in a landmark decision, the U.S. District Court for the Eastern of New York applied the Howey Test and determined that a federal indictment of Maksim Zaslavskiy sufficiently alleged that the transactions at issue involved securities. [211] On July 15, 2018, Zaslavskiy pled guilty and the government recommended a sentence 30–37 months imprisonment. [212] Following a superseding indictment to and subsequent plea, Zaslavskiy is awaiting sentencing.

In December 2017, the SEC brought enforcement actions involving the PlexCoin and Munchee ICOs for offering unregistered

securities. [213] As of June 2019, 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.

On September 11, 2018, the SEC entered an order finding that Crypto Asset Management LP (CAM) engaged in an unregistered nonexempt public offering and caused a fund to operate as an unregistered investment company. According to the order, CAM falsely marketed the fund as the "first regulated crypto asset fund in the United States," and falsely claimed that the fund was regulated by and registered with the SEC. Timothy Enneking, the sole principal of CAM, and CAM agreed to the SEC's cease and desist order and pay a penalty of $200,000. [214] This was the SEC's first enforcement action finding an investment company registration violation by a hedge fund manager based on its investments in digital assets.

On September 11, 2018, the SEC also announced that TokenLot LLC and its owners would settle charges that they acted as unregistered broker-dealers. TokenLot was promoted and operated as a means of purchasing digital tokens during ICOs and engaging in secondary trading. TokenLot and its owners agreed to pay over $520,000 combined in disgorgement, interest, and penalties. [215] This was the first case since the SEC's 2017 DAO Investigative Report in which it advised that those who offer and sell digital securities must comply with federal securities laws. [216]

On October 3, 2018, the SEC filed a complaint seeking to enjoin Blockvest, LLC and its founder from conducting an unregistered ICO. [217] The SEC alleged, among other things, that Blockvest had falsely claimed that its ICO had been registered and approved by the SEC. On November 27, 2018, the United States District Court for the Southern District of California issued an order denying the SEC's request for a preliminary injunction because the SEC had not provided sufficient evidence that Blockvest's tokens were securities. [218] However, several months later, the court reconsidered and reversed its prior order concluding that the SEC presented enough facts for the court to preliminarily enjoin Blockvest from further violating Section 17(a) of the Securities Act. [219] The court's opinion provides helpful analysis on what it means to "offer" securities in the context of crypto tokens and demonstrates that defendants can run afoul of securities laws simply by publishing a white paper and a website, without ever selling any functional tokens. This matter remains ongoing.

On November 8, 2018, the SEC settled its first case against an unregistered cryptocurrency exchange, EtherDelta. [220] EtherDelta operated on the Ethereum network, matching buyers and sellers of ether and "ERC20" digital assets. To settle SEC's charges EtherDelta's founder agreed to pay disgorgement and a civil fine.

In May 2019, the SEC filed a complaint for injunctive relief and obtained an order halting an ongoing $30 million Ponzi scheme in which Argyle Coin, LLC, a purported cryptocurrency business, promised to use investor funds to develop a cryptocurrency business. [221] This action remains ongoing.

In June 2019, the SEC filed a complaint against Kik Interactive Inc., creator of an online messaging application, for conducting an illegal $100 million securities offering of digital tokens. [222] The complaint alleges that Kik sold its "Kin" tokens to the public, and at a discounted price to wealthy purchasers, raising more than $55 million from U.S. investors. This action remains pending in federal court.

FINRA

On September 11, 2018, FINRA announced that it was taking its first disciplinary action in a case involving virtual currency.[223] It filed a complaint against Timothy Tilton Ayre of Agawam, Massachusetts. From January 2013 to October 2016, FINRA alleges that Ayre sought to have investors invest in his severely unprofitable public company, Rocky Mountain Ayre, Inc. (RMTN), through issuing and selling HempCoin, a product that he claimed was the "first minable coin backed by marketable securities." [224] According to FINRA, in June 2015, Ayre apparently bought the rights to HempCoin and "repackaged it as a security backed by RMTN common stock." [225] FINRA has charged Ayre with the unlawful distribution of an unregistered security and securities fraud for "making materially false statements and omissions regarding the nature of RMTN's business, failing to disclose his creation and unlawful distribution of HempCoin, and making multiple false and misleading statements in RMTN's financial statements." [226] FINRA's actions represents its stepped up presence among regulators closing watching the development of cryptocurrency markets.

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. [227]

Blake Benthall, who operated Silk Road 2.0, a follow-on site to Silk Road, was arrested in November 2014 on similar charges. [228]

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. [229]

Federal Trade Commission (FTC)

In March 2018, the FTC halted the activities of four individuals who promoted chain referral schemes and violated the FTC Act's prohibition against deceptive acts by misrepresenting the chain referral schemes as bona fide money-making opportunities and by falsely claiming that participants could earn substantial income by participating in the schemes. [230]

State enforcement

On May 21, 2018, the North American Securities Administrators Association (NASAA) announced a series of enforcement actions against fraudulent ICOs and cryptocurrency-related products coordinated between American state and Canadian provincial securities regulators. In May alone, the NASAA reported nearly 70 inquiries and investigations and 35 pending or completed enforcement actions. [231]

On March 27, 2018, the Secretary of State of the Commonwealth of Massachusetts announced it had ordered five firms to halt ICOs because they were selling unregistered securities. [232] On January 24, 2018, the Texas State Securities Board issued an emergency cease and desist order to R2B Coin, a Hong Kong entity, for allegedly issuing unregistered securities to Texas residents with false and misleading information. [233]

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 federal and state level.

International regulation of digital currency is fast evolving and will vary substantially across member states.

Chapter 6 **European financial regulatory landscape**

The treatment and characterization of cryptocurrency has not yet been fully clarified by European regulators. The European Securities and Markets Authority (ESMA), as well as several other national regulators in Europe, have published opinions on cryptocurrencies and have begun assessing how digital currencies fit into their regulatory perimeter. The European Union (EU) is working to adapt and update already existing AML and money transmission regulations to cover digital currencies. Some national regulators, including the UK, have also made the decision to further gold-plate these AML regulations.

Background

The European Court of Justice ruled in late 2015 that bitcoin and other digital currencies should be treated as a currency. This ruling stood in contrast to the U.S. CFTC's decision that treated digital currencies as commodities. It was thought that this ruling, along with a 2014 Opinion issued by the European Banking Authority (EBA) urging an EU-wide digital currency regulatory regime, could have the effect of unifying European regulation on the subject, which had varied more substantially from country to country. Certainly, in 2018, the ruling may be seen as having provided impetus for a Pan-European definition of virtual currency. However, the definition introduced by the Fifth Anti-Money Laundering Directive (MLD5) goes beyond the view put forward by the European Court of Justice (ECJ) and describes virtual currencies as a "means of exchange" rather than payment, beyond the sphere of traditional currency as we know it today.

During 2018 and 2019, the time that regulators across the EU have dedicated to ICOs has increased dramatically. [234]

As noted above, international regulation of digital currency is fast evolving and will vary substantially across member states. 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 – Status of virtual currency

October 2015 European Court of Justice ruling

In one of the first major digital currency court cases impacting the EU as a whole, on October 22, 2015, the ECJ held that bitcoin should be treated as a currency and means of payment for tax purposes. [235] This holding stands in contrast to regulation in the United States, in which the CFTC determined that digital currencies should not be treated as currencies, but instead as commodities (whereas the IRS treats digital currencies as property). [236]

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 VAT to tax "transactions, including negotiation, concerning currency, bank notes and coins used as legal tender." [237] 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. [238]

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.

MLD5: Virtual currency defined

More than two years after an initial proposal by the European Commission to incorporate virtual currency into the Europe-wide AML scheme, the EU enforced the MLD5. It broadly aimed to increase the transparency of new payment systems and, in doing so, incorporated "virtual currency exchanges" into its provisions.

Importantly, this is the first definition with the force of European legislation of a virtual currency. The new definition takes a not dissimilar view to the ECJ in its 2015 ruling, and certainly does not take the American position of classing digital currencies as commodities. Nonetheless, neither is it classed as a currency in the traditional sense.

MLD5 defines virtual currency as "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically." In being described as a means of "exchange" rather than "payment," the directive clearly differentiates between it and "currency." Virtual currency can only be traded in a limited sphere and is only accepted by pre-agreed traders as valuable consideration.

MLD5 gives a broad definition of a "virtual currency exchange." Although to qualify, an exchange must facilitate the exchange of virtual currency for fiat currency, this need not be its "primary and professional" activity, as was suggested in the Commission's 2016 proposal. This widens the range of services and businesses that might be caught by the provisions.

Custodian wallet systems also become regulated entities under this directive and are required to carry out customer due diligence, including KYC checks.

Member States have until January 10, 2020 to implement this directive, but the European Commission hopes to encourage early implementation.

The UK's FCA published a consultation in April 2019 on how the UK should transpose MLD5 into UK law, and in particular, whether MLD5 should be gold-plated. [239] The FCA has said that it is inclined to go beyond the provisions set out in MLD5 to ensure that the UK continues to fully address the money laundering/terrorist financing risks that are not covered by MLD5. The FCA will also attempt to mitigate the risk of cryptocurrencies being used in illicit activity. In its consultation, the FCA sought stakeholder views on whether activities, such as (i) crypto-to-crypto exchange service providers; (ii) peer-to-peer exchange service providers; (iii) crypto asset ATMs; (iv) the issuance of new crypto assets, through ICOs for example; and (v) the publication of open-source software, should be brought within the scope of MLD5.

Europe – Regulatory initiatives

European Banking Authority and the European Central Bank

In July 2014, the 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. [240] 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. [241] 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. [242]

In order to address the numerous risks of digital currency, the EBA's opinion advocated that "a substantial body of regulation" be implemented. [243]

The European Central Bank (ECB) 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. [244] 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. [245]

Consultation papers: ESMA and European Supervisory Authorities

European Securities and Markets Authority

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. [246]

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.

The ESMA chair Steven Maijoor told the European Parliament's economic affairs committee that ESMA would report on how best to regulate ICOs that do not fall within already established regulatory framework, by the end of 2018. [247]

More recently, in 2018, ESMA imposed temporary restrictions on selling, marketing, and distributing cryptocurrency contracts for derivatives (CFDs) to retail clients. [248] ESMA cited the significant concerns about investor protection across the EU as the reason for these restrictions.

ESMA concluded that CFDs with cryptocurrencies as the underlying asset raise significant concerns and noted that cryptocurrencies are a relatively immature asset that pose major risks for investors, particularly retail clients who do not understand the risks involved.

In January 2019, both ESMA and the EBA published advice to the European Commission, Council, and Parliament on ICOs and crypto assets. ESMA's advice clarified the existing EU rules that apply to crypto assets that qualify as financial instruments. ESMA concluded that the status of a particular crypto asset must be assessed separately for each token. It also gave ESMA's view on any gaps and issues in the EU financial regulatory framework for policymakers to consider. In particular, some of the risks that

are specific to the underlying technology of crypto assets are unaddressed in the existing regulatory framework. Furthermore, certain existing requirements are not easily applied, and may not be relevant, in a DLT framework. In this advice, ESMA noted its concern on the risks crypto assets poses to investor protection and market integrity. ESMA has highlighted that its preference is for an EU-wide approach to crypto assets. It is therefore likely that the EU will adopt a regulatory framework for crypto assets that do not qualify as MiFID II financial instruments.

IOSCO

The International Organization of Securities Commissions (IOSCO) published a board communication on concerns related to ICOs in January 2018 that focuses on the risks associated with trading crypto assets on crypto asset trading platforms. [249] ICOs are highly speculative investments in which investors are putting their entire invested capital at risk. IOSCO's comment that, although some operators are providing legitimate investment opportunities, the increased targeting of ICOs to retail investors through online distribution channels raises investor protection concerns.

IOSCO further notes that, in the event that a crypto asset falls within an IOSCO member's regulatory remit, it would expect that the existing regulatory frameworks apply to that asset and, subsequently, to the crypto asset trading platform.

Overall, the IOSCO consultation concluded that even in circumstances where a crypto asset is not a regulated product, the issues and risks posed by trading on a crypto asset trading platform are similar to those associated with trading traditional financial products. Consequently, IOSCO expects that its three core objectives – investor protection; ensuring markets are fair, efficient and transparent; and reduction of systematic risk – will apply.

FCA consultation papers

In January 2019, the FCA published a consultation on proposed guidance on crypto assets. [250] This guidance, built on recommendations made by the UK Cryptoassets Taskforce in October 2019[251] focused on where activities relating to different types of crypto assets do, or do not, come within the FCA's regulatory perimeter. The guidance also defined and described different types of crypto assets and their common features:

1. **Security Tokens:** Tokens that meet the definition of a Specified Investment under the FSMA Regulated Activities Order, like a share or a debt instrument, and fall within the regulatory perimeter. This will be determined by its intrinsic characteristics and the contractual rights and obligations the token-holder has, such as contractual entitlement to profit-share through dividends or ownership.
2. **Exchange Tokens:** Tokens that are not issued or backed by any central authority and are meant and designed to be used as a means of exchange. They are, usually, a decentralized tool for buying and selling goods and services without traditional intermediaries. Bitcoin is an example of such tokens. They do not currently fall within the FCA's regulatory perimeter.
3. **Utility Tokens:** These typically grant holders access to a current or prospective product or service but do not give the same rights as those granted by Specified Investments. Utility tokens can also meet the definition of e-money, in which case activities in relation to them may be within the regulatory perimeter.

The FCA have said that the potential benefit to retail consumers from this ban would range from £75 million to £234.3 million a year

Proposed retail ban

On July 3, 2019, the FCA published a consultation in which it proposed banning the sale of derivatives and exchange traded notes (ETNs) referencing certain types of crypto assets to retail consumers. [252] This proposal follows a number of FCA statements and papers relating to crypto assets, their regulatory treatment, and their effect on markets.

In its consultation, the FCA said that retail consumers are unable to reliably assess the value and risks of derivatives and ETNs referencing unregulated transferable crypto assets due to the nature of the underlying assets, which have no inherent value. In particular, the FCA cites the prevalence of market abuse and financial crime in the secondary market for crypto assets and the extreme volatility in crypto asset price movements as risks that retail consumers may be unable to assess. Furthermore, the FCA suggested that there is also a lack of a clear investment need for products referencing crypto assets

The ban will encompass the sale, marketing, and distribution to all retail consumers of all derivatives, including CFDs, options and futures, as well as ETNs that have crypto assets as the underlying commodity.

The FCA have said that the potential benefit to retail consumers from this ban would range from £75 million to £234.3 million a year.

Crypto asset perimeter guidance

On July 31, 2019, the FCA also published its final guidance on the types of crypto assets that fall within the FCA's current regulatory framework. [253] This clarifies the resulting obligations for firms and regulatory protections for consumers. The guidance sets out where tokens are likely to be Specified Investments under the Regulated Activities Order; e-money under the E-Money Regulations; captured under the Payment Services Regulations; or outside of the regulatory perimeter. The guidance also creates a new category of regulated "E-Money Tokens." This category is distinct and therefore separate from the utility tokens and security tokens category. This guidance makes it clear that firms carrying on certain specified activities in relation to crypto assets must obtain the appropriate authorizations.

This represents the most significant regulatory developments in the UK through Summer 2019. Please see the specific UK section below for more historic developments.

Europe – Legislation

Digital currency and AML legislation

As noted above, on June 19, 2018, the text for MLD5 was published in the Official Journal of the European Union. MLD5 entered into force on July 9, 2018. The directive has brought certain virtual currency services within the scope of the European AML framework, realizing an action plan adopted by the European Commission over two years prior to adoption.

One of the aims of MLD5 is to increase transparency in newly developed payment methods and thereby bring virtual currencies into the scope of European AML regulation. The new language consequently expands the existing directive to cover "virtual currency exchanges" and "custodian wallet providers," with the result that these businesses will need to carry out customer due diligence on prospective clients. The directive is perceived by many to narrow the gap between the United States and the EU for digital currency exchange platforms and custodian wallet providers. The deadline for Member States to implement the provisions of this directive is January 10, 2020, though the European Commission is encouraging earlier implementation.

The first EU definition of virtual currency

Significantly (and as noted above), MLD5 provides the first EU definition of virtual currency and is set out below:

"A digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically."

The definition means that a token which: (i) is not accepted by any merchant or individual as a means of payment for goods or services; and (ii) may only be exchanged on a limited number of virtual currency exchanges, may still be caught, as it would be difficult to argue that an integral characteristic of any token is not its exchangeability. Indeed, Recital 10 of MLD5 states that "although virtual currencies can frequently be used as a means of payment, they could also be used for other purposes and find broader applications such as means of exchange, investment, store-of-value product or use in online casinos." It appears that this definition was created to cover any coin or token issued through an ICO, notwithstanding its inherent features – a sentiment prevalent in the MLD5 preamble, which states that "the objective of this directive is to cover all the potential uses of virtual currencies."

E-money

MLD5 also makes it clear that virtual currency should not be confused with e-money (as defined in article 2(2) of Directive 2009/110/EC (the E-Money Directive)) or funds (limited to meaning banknotes and coins, scriptural money or electronic money, as defined in point 25 of article 4 of Directive (EU) 2015/2366 (the Payment Services Directive). The potential categorization of ICOs as e-money issuance has been a hot topic of debate around Europe for some time. The step toward regulatory clarity in this regard will be welcomed.

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. [254]

Notable European nations that many view as having less stringent digital currency regulation include the UK and Switzerland (although note that Switzerland, and perhaps soon the UK, is not in the EU). Many believe the UK 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 UK. See further detail on the FCA's regulatory sandbox below.

In addition, many European regulators have piloted new regulatory initiatives to encourage innovation in this area. This includes the French Autorité des marches financiers (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 POC face to real-life deployment, for example, the use of blockchain on the Lantmäteriet, the Swedish land registry. [255]

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. [256] 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. [257]

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. [258] 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." [259]

France

France's Minister of the Economy and Finance requested in March 2018 that a draft proposal for a legislative framework to regulate digital currencies be drawn up. The legislation, accepted by the French government in September of that year, enabled France's stock market regulator, AMF, to give licenses to companies to issue ICOs to raise funds, upon the application of that company.

Additionally, in September 2018, France's data protection authority Commission Nationale de l'informatique et des Libertés (CNIL) released guidance on how to apply the General Data Protection Regulation (GDPR) to blockchain technologies. Although the paper is a welcome development, it asks more questions than it answers. We see the convergence of data law and blockchain as a key theme in this space over the coming months and years.

More recently, in April 2019, the French National Assembly adopted an Action Plan for Business Growth and Transformation. This action plan will establish a framework for cryptocurrency-based fundraising and for digital asset services providers. If blockchain companies opt into the regulation, this new law will grant these companies the right to a bank account. To opt in, companies must obtain a license from the French regulatory authority. In the event that blockchain companies decide not to opt in, they will be prohibited from solicitation, patronage, and sponsorship activities.

Germany

The Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)) has historically displayed a cautious approach to cryptocurrencies. It was among the earlier European regulators to declare bitcoin a unit of account and as such a financial instrument subject to regulation depending on the circumstances of the case. [260] In March 2018, BaFin published an advisory letter on the classification of tokens as financial instruments, emphasizing the regulated nature of crypto tokens that display the characteristics of securities or other regulated products. [261] An attempt was made in late 2018, by the Higher Regional Court of Berlin, to argue that bitcoins do not constitute units of account, when it was tasked with deciding the question

of whether the operation of a bitcoin trading platform without a license from BaFin constituted a criminal offense. [262] Despite this attempt, it has come as no great surprise that the year 2019 saw the publication of a draft legislative proposal to create a new residual category of financial instrument, namely that of "crypto-assets." [263]

The legislation was prompted by the need to implement MLD5 into national law by January 10, 2020. Instead of just imposing the obligations arising from the German Money Laundering Act (Geldwäschegesetz (GWG")) on virtual currency exchanges and custodian wallet providers as envisaged by MLD5, the German Ministry of Finance, in its draft law, opted to create a new regulated activity – "crypto custody business." This is done by expanding the list of financial services contained in the German Banking Act (Kreditwesengesetz (KWG)). Crypto custody business is described as being "the custody, administration and safekeeping of crypto assets or private cryptographic keys used to hold, store and transfer crypto assets, for others" (non-official translation).

In deviation from the "virtual currencies" terminology used in MLD5, the German legislator has opted for the term "crypto assets." The proposed definition of "crypto assets" is close to that given to virtual currencies in MLD5, save that the "digital representation of value" would be caught by the legislation not just when used as a means of exchange (or payment) but also "for investment purposes." This means that not only cryptocurrencies and payment tokens would constitute financial instruments but also investment and security tokens.

The practical consequence of the proposed change is that not just the provision of wallet services in respect of crypto assets or the operation of a virtual currency exchange, but also carrying out on a commercial scale any of the regulated activities listed in the KWG, such as proprietary trading, operating a multilateral trading facility, investment broking or asset management, could constitute a regulated activity requiring BaFin authorization. A person providing financial services without the necessary authorization will usually be ordered to immediately cease business operations and may be punished by a fine or a term of imprisonment of up to five years (Sections 37 and 54 para. 1 No. 2 in conjunction with Section 32 para. 1 KWG).

It should also be kept in mind that persons engaging in such regulated activities would be subject to the KYC, reporting and other AML and contra terrorist financing obligations arising from the GWG.

The proposed changes are part of a broader goal set by the German government of developing a blockchain strategy and creating a suitable regulatory framework for crypto assets. In Q1 2019, a public consultation on blockchain was launched. The government has taken a holistic view of the technology, analyzing technical, economic, and legal opportunities and challenges. It has also considered blockchain in a sector-specific context, including the financial sector, energy, Internet of Things technology (IoT), and supply chains, to name but a few. At the time of publication of this white paper the results of the public consultation have yet to be released.

Italy

Exactly one year after the European Commission adopted its 2016 proposal, the Italian AML Decree, which implements MLD4, came into force. [264] Among other things, the decree brought "digital currencies" and "digital currency services" within the scope of Italian AML laws. It correctly anticipated that the European Parliament would vote on the proposals to bring digital currencies within the scope of MLD4 in 2018. Indeed, all Member States are now required, under MLD5, to bring digital currency within the scope of their respective national regimes.

In January 2019, the Italian Senate committees of Constitutional Affairs and Public Works approved an amendment to the Italian AML Decree. This amendment defines distributed ledger technology-based technologies and smart contracts. The amendment would give legal effect to blockchain-based registers of the memorialization of documents. This is now awaiting the approval of the Italian Parliament before it becomes law.

The UK

As noted above, the UK FCA has issued various warnings regarding the risks associated with investing in digital assets such as bitcoin and ether. Specifically, the FCA has warned investors that: (a) cryptocurrencies are not issued or guaranteed by a central bank or public authority; (b) cryptocurrencies do not have any legal status as a "fiat currency"; and (c) the purchase and sale

of cryptocurrencies are not subject to safeguards and protections as they are unregulated in the UK. [265]

Further, in March 2018, the UK Government announced plans for a "cryptocurrency task force" to investigate the risks and benefits of cryptocurrencies and to examine how blockchain can be exploited by the wider financial sector. At the same time, it announced its initiative in "robo-regulation" – the use of software to carry out parts of the regulatory process. The UK Chancellor of the Exchequer has also said he plans to establish new industry standards to remove barriers to fintech companies that want to partner with banks by creating "shared platforms" on which firms can set up new systems.

Regulatory sandbox

On July 3, 2018, the UK FCA announced that 29 firms had successfully been accepted into its regulatory sandbox, 11 of which are blockchain-related start-ups. The sandbox is designed to enable such start-ups to test their ideas, projects, and solutions in the UK market under a controlled regulatory environment. In addition (and following an initial proposition by the UK's FCA in February 2018 on the idea of a "global sandbox"), a GFIN was established in August 2018 to create a network of global regulators that promotes innovation and knowledge sharing on emerging innovation trends. Regulators involved in the GFIN include the French AMF, the Singapore Monetary Authority of Singapore (MAS), and the UK FCA. [266]

UK Crypto Taskforce

In addition, in March 2018, the UK Government launched the Cryptoassets Taskforce consisting of HM Treasury, the FCA and the Bank of England. The taskforce's final report (CATF Report) was published in October 2018. [267] This set out the UK's policy and regulatory approach to crypto assets and made a number of commitments. The CATF Report committed to mitigate the risks that crypto assets posed to consumers and market integrity; prevent the use of crypto assets for illicit activity; guard against potential, emerging threats to financial stability; and encourage the responsible development of legitimate DLT and crypto asset-related activity in the UK. Furthermore, HM Treasury committed to broaden the scope of UK AML legislation and consult on crypto assets that are currently outside of the UK's regulatory perimeter. Finally, the FCA committed to consult on a potential ban on the sale to retail consumers of derivatives referencing certain types of crypto assets and guidance clarifying the types of crypto assets that already fall within the current regulatory perimeter.

As noted above, this year (2019), the FCA has published a consultation on the ways in which UK AML legislation should gold-plate MLD5 and has also published a consultation proposing to ban the sale of crypto assets to retail consumers, as well as guidance on the regulatory status of certain crypto assets.

Europe ICO "friendly" jurisdictions

Jersey

On September 26, 2016, the Proceeds of Crime (Miscellaneous Amendments) (Jersey) Regulations 2016 came into effect. [268] 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 (JFSC).

The regulations define virtual currency as "any currency which (while 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 JFSC aims to treat virtual currency as a currency, as opposed to a commodity, regulating these new currencies within an existing statutory regime.

JFSC issued a guidance note in 2018 in which it detailed its new application process for the issuers of ICOs. JFSC noted that most ICOs are unlikely to be regulated, however, there are certain requirements that ICO issuers based in Jersey must follow to maintain regulatory compliance. The guidance also provides a description of the different classifications of ICOs. ICOs are split into "security tokens" and "non-security tokens." JFSC has specified that utility and cryptocurrency tokens will fall into the "non-security tokens" bracket for regulatory purposes.

Gibraltar

The Gibraltar Financial Services Commission in February 2018 announced that it was developing a draft law to regulate ICOs – possibly the first such regulation of its kind in the world. It will introduce the concept of "authorized sponsors" to ensure "compliance with disclosure and financial crime rules."

Malta

In June 2018, the Maltese Parliament approved three bills, entitled the "Innovative Technology Arrangements and Services Act," the "Virtual Financial Assets Act," and the "Malta Digital Innovation Authority Act." They provide for the regulation of ICOs and establish the powers of the Malta Digital Innovation Authority, which will primarily be in charge of developing and promoting the blockchain industry in Malta.

The European Commission has recommended that Malta increase its AML enforcement efforts to ensure it continues to effectively regulate its growing crypto and gaming industries. The European Commission has also requested that Malta look at its tax system to prevent aggressive tax planning and tax avoidance.

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." [269]

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.

In 2018, FINMA announced new requirements for blockchain companies applying for a fintech license in Switzerland. The new requirements are notably less restrictive than those imposed on incumbent financial services companies. FINMA has stated that its goal is to facilitate greater market access for fintech companies and boost innovation within Switzerland.

Chapter 7 **Asian financial regulatory landscape**

Asian regulatory landscape

While Asian countries have generally been open toward DLT, regulatory responses to cryptocurrency have varied across the region. At one end of the spectrum, China has taken steps to restrict the use of digital currencies, while at the other end, Japan continues to encourage their development. Many jurisdictions in the region have taken steps to address risks of fraud and money laundering associated with the use of digital currencies.

Singapore

Singapore has evolved to become a popular destination for businesses involved in cryptocurrency. The MAS, the country's central bank and financial regulatory authority, has been keen to position Singapore as a jurisdiction that is open to innovation but imposes appropriate safeguards where needed to counter resulting risks.

The MAS acknowledges the potential of DLT, and has undertaken a series of trials (referred to as Project Ubin [270]) to test the application of this technology to interbank payments and transaction settlement, focusing on methods for tokenization of currency and securities, automation of delivery versus settlement, interoperability between different ledgers (including on a cross-border basis), and settlement finality.

The MAS is also introducing a new payment services framework, in the form of the Singapore Payment Services Act. [271] Scheduled to take effect by early 2020, the Payment Services Act consolidates and replaces Singapore's existing legislation in this area and aims to establish a proportionate, risk-based framework that will apply to designated payment systems and providers of payment services such as remittance, money-changing, merchant acquisition, and e-money issuance firms. In the DLT space, firms most likely to become subject to the Payment Services Act are cryptocurrency dealers and exchanges, which will henceforth be subject to a specific licensing and conduct regime.

However, the use of cryptocurrencies such as bitcoin and ether as a means of payment or investment by any other person (not acting as an intermediary) is not subject to any restriction. As recently as July 2019, Singapore's tax authority, the Inland Revenue Authority of Singapore, published a draft proposal [272] seeking to exempt the use and exchange of cryptocurrencies from goods and services tax, starting January 1, 2020.

Japan

Following the 2014 collapse of Japan-based Mt. Gox, Japan moved to amend its Payment Services Act in 2016 to protect consumers and better regulate cryptocurrencies. In April 2017,[273] Japan officially recognized bitcoin and other digital currencies as "Virtual Currency" that possesses proprietary value under its Payment Services Act and is capable of being used for payments. Under the same Act, business operators involved in "Virtual Currency Exchange Services" have to be registered with Japan's Financial Services Agency (FSA). As of January 2018,[274] the FSA had approved 16 Japanese cryptocurrency exchanges.

Despite the regulations, in January 2018, Coincheck, one of Japan's largest cryptocurrency exchange businesses, suffered a loss of approximately US$530 million from hackers. [275] The FSA, in cooperation with Japan's Consumer Protection Agency and the National Police Agency, then commenced inspections of cryptocurrency exchanges and released an interim report in August 2018 highlighting poor business operations and controls.[276] In late 2018, the FSA granted the cryptocurrency industry self-regulatory status, permitting the Japan Virtual Currency Exchange Association to police and sanction exchanges for any violations. [277]

Taiwan

As early as 2013, the Central Bank of the Republic of China (Taiwan) and Taiwan's Financial Supervisory Commission (FSC) issued a joint statement warning that bitcoin is not a currency but a highly speculative digital "virtual commodity" (the 2013 Notice).[278] This was followed by a FSC notice prohibiting banks and financial institutions in Taiwan from accepting or exchanging bitcoin, or providing bitcoin-related services at bank ATMs (the 2014 Notice). [279]

The FSC reiterated the 2013 Notice and 2014 Notice in 2017, stating that bitcoin is a speculative virtual commodity and that financial institutions should not participate in or provide services or transactions relating to virtual currencies. The FSC also elaborated on its position regarding ICOs, stating that they could be covered under securities regulation and warning that any illegal activities such as fraud would be sanctioned in accordance with the law.

In November 2018, [280] Taiwan's Money Laundering Control Act was amended to include virtual currency platforms within its scope.

More recently, in June 2019, [281] in what is considered a world first, the FSC released draft regulations on security token offerings (STOs) for public consultation. Unlike other jurisdictions that require STOs to comply with existing securities laws, the new regulations are catered specifically to STOs. The regulations are intended to allow private companies registered in Taiwan to conduct both local and foreign STOs, subject to a NT$30 million fundraising limit.

Hong Kong

The Hong Kong Securities and Futures Commission (SFC) published its regulatory approach to virtual assets in November 2018. [282] Prior to this statement, markets for virtual assets were not subject to SFC oversight if the virtual assets were not within the definition of "securities" or "futures contracts." The SFC had previously issued warnings on cryptocurrencies and taken regulatory action against cryptocurrency exchanges and issuers of ICOs for dealing in cryptocurrencies which are "securities." [283]

However, the SFC noted the increasing exposure of investors to virtual assets and their accompanying risks. As such, the SFC has expanded its mandate to regulate virtual asset portfolio managers and fund distributors (subject to a de minimis requirement of 10 percent or more of gross asset value of the portfolio being invested in virtual assets), and these portfolio managers and fund distributors must be registered or licensed with the SFC, and comply with the SFC's requirements. Such requirements include dealing only with "professional investors," as defined under the Hong Kong Securities and Futures Ordinance.

The SFC has also set out a regulatory framework [284] for the potential regulation and licensing of cryptocurrency exchanges. The SFC proposes that cryptocurrency exchanges may voluntarily enter into its regulatory sandbox by offering one or more virtual assets that would fall under the definition of "securities" on its platform and hence fall under SFC regulation.

China

In China, cryptocurrencies threaten to undermine its capital controls. While mere use of bitcoin and digital currencies by individuals has not yet been declared punishable, its use has become increasingly difficult, if not impossible, due to numerous regulations in place.

In 2013, [285] the People's Bank of China (PBoC), the Ministry of Industry and Information (MIIT), the China Banking Regulatory Commission (CBRC), the China Securities Regulatory Commission (CSRC), and the China Insurance Regulatory Commission (CIRC) jointly issued a notice on the 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.

In 2017, [286] the PBoC, Office of the Central Leading Group for Cyberspace Affairs, the MIIT, the State Administration of Industry and Commerce, 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 involve illegal offering of tokens, illegal offering of securities, illegal fundraising, financial fraud, Ponzi schemes, and similar criminal offenses. Platforms for token financing and trading are prohibited from (1) exchanging legal tender for tokens, "virtual currency" or vice versa; (2) buying or selling or acting as central counterparty for tokens or "virtual currency;" or (3) providing pricing or information services for tokens or "virtual currency."

In the wake of the 2017 Notice, various media outlets reported regulators shutting down cryptocurrency trading platforms. China has aggressively sought to curb access to cryptocurrency by restricting all banking or funding to cryptocurrency activity, [287] as well as blocking access to foreign platforms. [288] Bitcoin mining firms were also compelled by local authorities to reduce their operations in early 2018, [289] and the National Development Reform Commission in April 2019 issued guidelines that suggest mining could be banned altogether. [290]

Chapter 8 **Rest of the world financial regulatory landscape**

Blockchain – The Middle East

Although the Middle East is synonymous with oil and luxury tourism, the region, and in particular the United Arab Emirates (UAE), has strong technological foundations in place to create the world's first smart city. One notable type of technology that the UAE is pursuing to help achieve this is blockchain. For example, in 2016, His Highness Sheikh Hamdan bin Mohammed Al Maktoum launched the Dubai Blockchain Strategy; and in April of 2018, the UAE government launched the Emirates Blockchain Strategy 2021. The strategy aims to capitalize on the blockchain technology to transform 50 percent of government transactions into the blockchain platform by 2021. Further, the UAE Global Blockchain Council was established in February 2016 to explore and discuss current and future applications of blockchain. The council now consists of 46 members and are made up of key players in the blockchain industry – from government entities to international private companies.

Despite the underlying blockchain technology being welcomed and pursued within the UAE, cryptocurrencies in general, and bitcoin in particular, are experiencing more of a mixed reception. As such, there is a paucity of legislation and regulations specifically covering cryptocurrencies. Most of the financial regulatory authorities have warned against the inherent risks of virtual currencies and some are considering draft regulations. As of June 2019, however, only one regulator has issued a regulatory framework for cryptocurrencies (discussed below).

Under the UAE's Regulatory Framework for Stored Values and Electronic Payment Systems, "virtual currency" is defined as "any type of digital unit used as a medium of exchange, a unit of account, or a form of stored value." The regulation then expressly states that "all virtual currencies (and any transactions thereof) are prohibited." In a public statement, the governor of the UAE Central Bank explained and clarified that "these regulations do not cover cryptocurrencies and do not apply to bitcoin or other digital currencies, currency exchanges, or underlying technology such as blockchain." [291] 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.

The UAE has a number of free zones, with Abu Dhabi Global Markets (ADGM) and Dubai International Financial Centre (DIFC) being the most prominent. These free zones have their own laws (subject to few federal-level laws such as criminal and AML laws) and their own regulator. For instance, the Financial Services Regulatory Authority (FSRA) and the Dubai Financial Services Authority (DFSA) regulate financial activities within the ADGM and DIFC, respectively.

After a consultation in May 2018, the ADGM issued its framework to regulate cryptocurrencies under the auspices of the Financial Services and Markets Regulations of 2015 (FSMR), regulated by the FSRA. These amendments created a new regulated activity (Operating a Crypto Asset Business (OCAB)). The framework addresses the risks and issues around the trading of crypto assets and their impact on financial stability, consumer protection, and market abuse. OCAB permits undertaking of one or more "crypto asset" (as defined below) activities, which include, among other things: (i) buying, selling, or exercising any right in accepted crypto assets; (ii) managing accepted crypto assets belonging to another person; (iii) marketing of accepted crypto assets; and (iv) operating a crypto asset exchange. The framework defines crypto assets as a digital representation of value that can be digitally traded and functions as a medium of exchange and/or a unit of account and/or a store of value, but it does not have legal status in any jurisdiction. Any "accepted crypto assets" are those crypto assets that fulfill criteria prescribed by the FSRA. The fees for OCAB are comparatively higher than most other regulated activities within the ADGM. In addition to the fees applicable to crypto asset exchanges, a trading fee is levied on such exchanges, which is payable on a monthly basis. Although the ADGM has stated that it

Emirates Blockchain Strategy 2021 aims to capitalize on the blockchain technology to transform 50 percent of government transactions into the blockchain platform by 2021

does not intend to make a list of accepted crypto assets publicly available, it will, however, provide information to applications, and it has a non-exclusive list of factors that it will take into consideration. These include security, traceability, exchange connectivity, market demand/volatility, type of distribution ledger, innovation, and practical application. This, together with published guidance on crypto assets, makes the ADGM an attractive option for a cryptocurrency business in the UAE and the Middle East.

In the DIFC, the DFSA issued a statement in 2017, stating that it does not regulate cryptocurrencies and considers them to be high risk. The DFSA is believed to be considering regulating cryptocurrencies and regulatory developments may appear in the near future.

The UAE Securities and Commodities Authority (SCA), the governmental body that regulates UAE's financial and commodities markets, initially warned investors against token-based fundraising activities. However, toward the end of 2018, the SCA announced that it would issue a regulation to govern ICO and STOs and determine the status of coins and tokens in mainland UAE. The regulation is yet to be issued. However, the ADGM, through the FSRA, issued its own guidance to investors proposing to invest in ICOs and STOs – "Regulation of Initial Coin/Token Offerings and Virtual Currencies under the Financial Services and Markets Regulations." The ADGM has its own legal and regulatory requirements regarding raising funds through ICOs and STOs. The ADGM would need to deem any securities token to be a security for the purposes of FSMR. Any potential issuer would need to first apply to the authority to deem their token a security and demonstrate to the regulator that what they intend to offer has the characteristic of one of the security types that is highlighted in FSMR.

Outside of the free zones, 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 or a security, then its regulation would 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.

Elsewhere in the Middle East, in the Kingdom of Saudi Arabia, although bitcoin is illegal, digitization is at the forefront of the nation's vision of developing a vibrant digital economy by 2030. For example, in February 2018, the Saudi Arabian Monetary Authority signed an agreement with Ripple, a real-time gross settlement system, to help banks in Saudi Arabia improve their payments infrastructure. [292] This partnership, founded on blockchain technology, will enable users to instantly settle payments sent in to and out of the country with greater transparency and lower costs. Further, a pilot scheme successfully concluded at the end of 2018 between the Saudi customs authority's trade platform (FASAH) and with IBM's and Maersk's platform, TradeLense. [293] Used together, these trading platforms connect all stakeholders involved in cross-border trade and serve as the foundational base for a whole host of digital supply chains.

The Central Bank of Kuwait confirmed in January 2018 that it was creating an infrastructure for the issuance of an e-currency (which it distinguishes from virtual currencies). The bank's governor, Dr. Mohammad Y. Al-Hashel said, "In case the Central Bank of Kuwait decides to issue digital currency in the future, we will have the tools ready to go live." However, in terms of timing, the governor warned that "while it is right to demand speed of service, it must be remembered that some things need time" and "shortcuts are not the answer." [294]

In December 2018, the Kingdom of Bahrain central bank issued draft proposals to create "a regulatory framework for licensing and supervision of crypto-asset services." Pending formalized

regulations, the central bank launched a regulatory sandbox earlier this year to allow blockchain and crypto companies to work in the country. [295] Over 30 companies have now been approved – ranging from crypto exchanges to robo-advisors. According to the central bank, the sandbox allows firms to "test their technology-based innovative solutions relevant to fintech or the financial sector in general." The duration of the sandbox is up to nine months, with an option to extend it for up to three months.

Oman has also made progress in its blockchain usage and development. The country has created two platforms with a strategic focus on innovation and national growth. Similar to Bahrain's sandbox, Oman's "Blockchain Factory" (also known as Blockchain as a Service) allows start-ups and small and medium-sized businesses (SMEs) to explore its blockchain in a controlled environment. After development, the blockchain technology is gradually introduced to both the private and public sectors in Oman. The second platform, the "National Private Permissioned Platform," allows mature and production-ready blockchain applications and solutions to be used nationwide.

Known as the "World's Start-up Nation," Israel is now home to more than 200 blockchain start-ups. The country, driven by a strong defense industry, military, and cutting-edge academic institutions, has become a hub for start-ups and hi-tech innovation. The country's unique experience with fintech, cybersecurity, and cryptography has positioned Israel as a fount of blockchain innovation.

In Iran, all financial institutions are prohibited from handling cryptocurrencies, after an announcement by the Central Bank of Iran (CBI) in April 2018. Before the ban was announced, the CBI was considering the adoption of a national virtual currency, with senior members of the CBI believing that the blockchain system and cryptocurrencies will eventually replace the current system – a view shared by Masoud Khatouni, the deputy for information technology and communications network at Iran's biggest bank, Bank Melli Iran (BMI), who has stated that cryptocurrencies are "currently shaping the future of banking" and should be used by the banks themselves.

Most of the financial regulatory authorities have warned against the inherent risks of virtual currencies and some are considering draft regulations.

Chapter 9 **Insuring digital currency and digital currency business**

Companies that service the digital currency industry and its holders face risks unique to the digital currency [297] 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 and technology services liability (E&O) insurance. At least one U.S. court has characterized bitcoin as equivalent to traditional assets like "money" or "securities." [298] Similarly, the IRS has concluded that digital currency should be considered "property" under the Internal Revenue Code, [299] and the CFTC treats bitcoin and other virtual currencies as "commodities" for regulatory purposes.

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

But novel issues abound because of the unique characteristics of digital currency (and, for example, derivatives). Unlike most "traditional" currencies, bitcoin requires no governments or 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. [301] The possibility remains that governments will (indeed, some have) impose substantial regulatory burdens or penalties on companies operating within the industry, including the risk of fines, application of AML 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

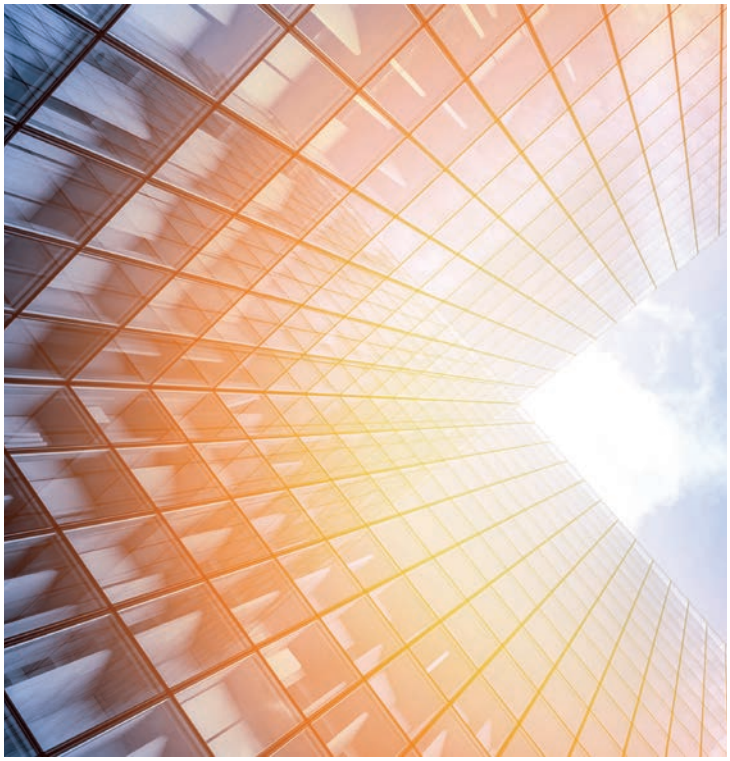
The digital currency industry continues to seek consensus on how best to secure bitcoin and other cryptocurrencies, as well as the companies that service digital currency holders, including storage companies, trading platforms, and exchanges. Ownership of digital currency is synonymous with knowing a 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 methods include "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 and malware 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, investigation 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. 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 private and regulatory 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.[302]

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. [303] 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. [304] 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. [305] Coverage for virtual currency may 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. [306]

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. [307] 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.

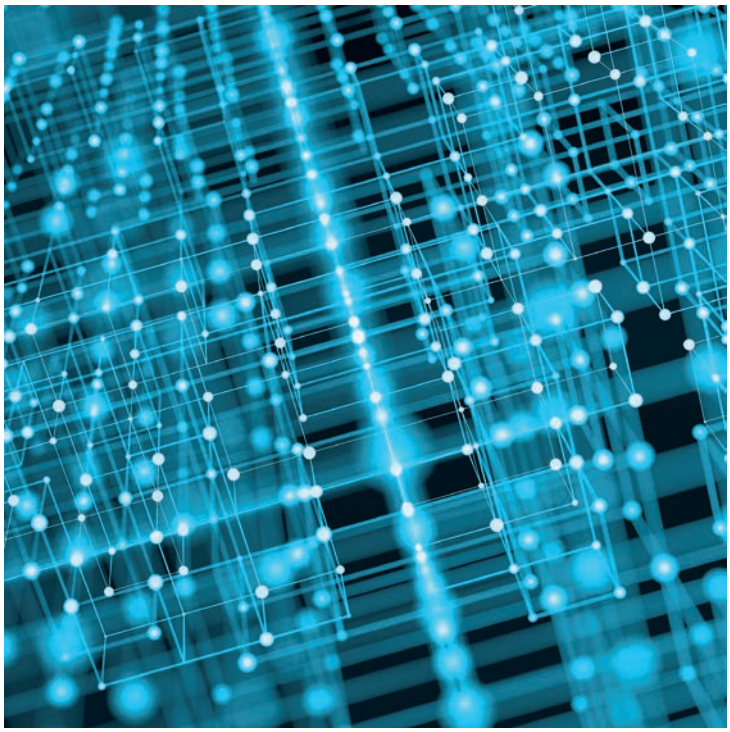
Based on public court filings, Bitpay and its insurer appear to have reached a settlement before any substantive rulings were made on the coverage issues raised in the case. Recent decisions from other courts, however, highlight a continued split in the case law on whether social engineering attacks are covered as "direct loss" under traditional fidelity or commercial crime policies. [308] For this reason, businesses should consider adding a specific social engineering fraud endorsement to their crime policy, which is now offered by several insurers. [309]

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 their 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 they may be tailored to specific risks; and thus, the definition of "professional services" may or may not automatically include such services.

companies performing bitcoin-related services should carefully review the way in which their E&O insurer defines covered professional 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 (that is, 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-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."

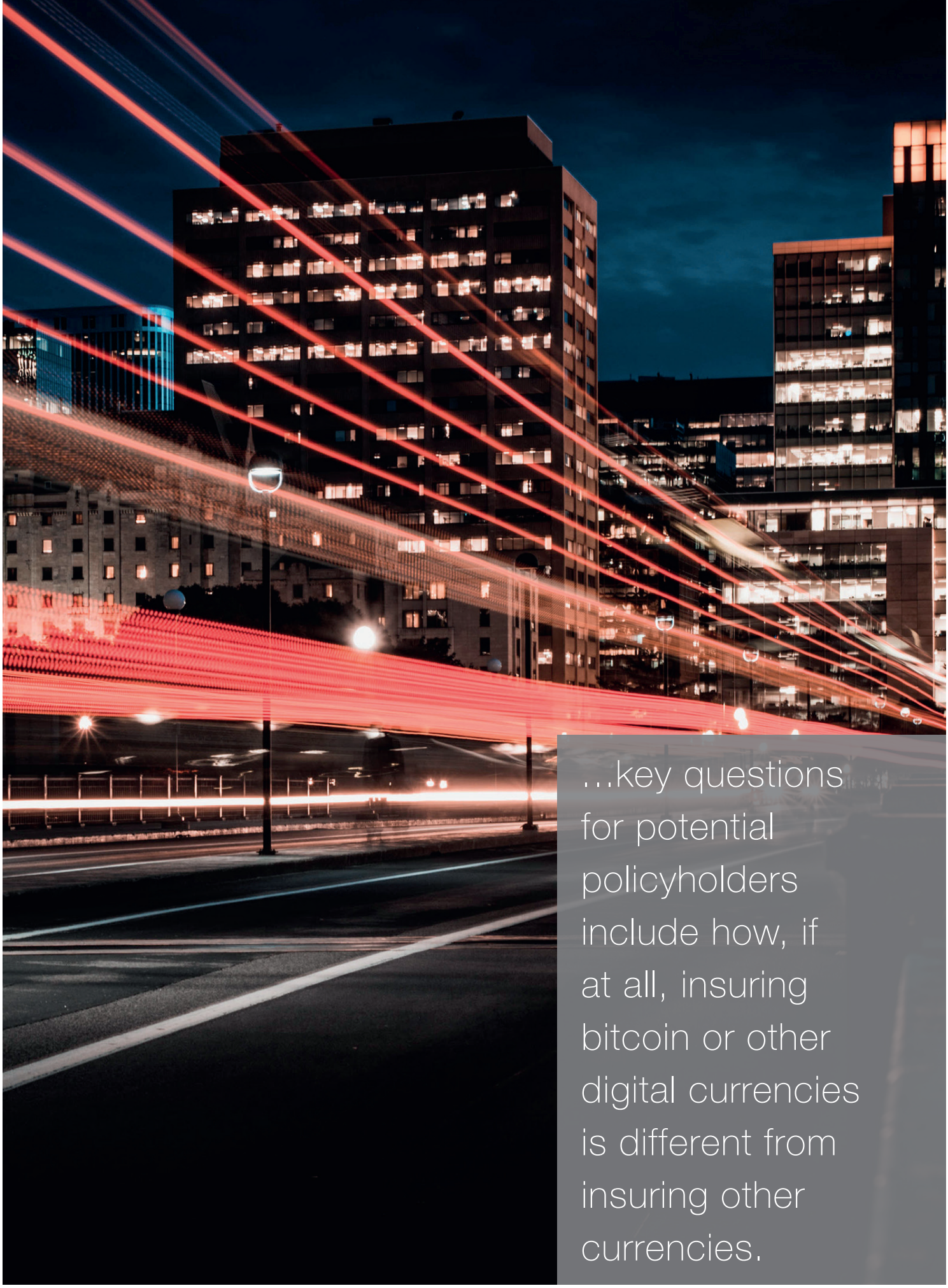
Bitcoin-specific insurance

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; [310] and another has developed a "new" type of commercial crime coverage specific to bitcoin. [311]

Other companies have created captive insurance funds to protect their customers instead of turning to insurance companies. [312] 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.



…key questions for potential policyholders include how, if at all, insuring bitcoin or other digital currencies is different from insuring other currencies.

Chapter 10 **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. [313] Several tech start-ups, 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. [314]

Some analysts are hailing blockchain technology as transformative, with Accenture describing it as possibly the "critical backbone" of the future capital markets infrastructure [315] and The New York Times describing it as a "fundamentally new way" of transacting and maintaining records. [316] 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 process of reviewing the technology within their firms. [317]

A separate survey from Greenwich Associates found that as much as $1 billion was invested in blockchain initiatives related to capital markets in 2016, [318] up from an estimated $75 million in 2015, according to consultancy firm Aite Group. [319]

Although 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 and more streamlined settlement, improved credit risk management 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, because 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. [320] Additionally, the potential savings for other transactions is even greater. For example, the average bank loan took nearly 19 days to settle in 2016. [321]

Initially, the blockchain is most likely to impact asset transactions where there is no central clearing or trading authority, such as transactions involving Fixed Income Clearing Corporation (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.[322] 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.[323] 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,[324] and in April 2017, as a member of a working group of seven firms, successfully tested blockchain and smart contracts to manage post-trade life cycle events for standard North American single-name credit default swaps. [325]

In addition to improved efficiency, the security provided by the blockchain may have an even greater impact on markets with high transaction volume, but minimal 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" consortium, using IBM to develop their blockchain-based trade financing platform.[326] The platform aims to fill financing gaps hampering domestic and cross-border trade for 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,[327] 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 DLT.

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 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 (as of then) the largest dollar amount ever raised for DLT.

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 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 and surpassing 500 as of October 2018. On October 1, 2018, the EEA and Hyperledger, Linux Foundation's collaborative project for open-source blockchain platforms, announced that they have formally joined each other's organizations to change the misconception that the two organizations are competitors and to further accelerate the adoption of blockchain technology for businesses.

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, 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; 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 when shares of a company are offered to the general public for the first time, a 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 Wilhelm 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 ether, and you get some of Billy's New Super Great Coin." [328] 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.

Token sales have been successful to varying degrees over time. From January 1, 2017 to July 26, 2017, blockchain entrepreneurs raised nearly $1.4 billion through token sales, [329] as compared with approximately $347 million raised through traditional venture capital funding during the same period. [330] On June 20, 2017, $95 million was raised through the sale of tokens by status for its browser, wallet, and messaging app. [331] In another token sale offered by the Bancor Foundation, $153 million was raised in just three hours. [332] Not to be outdone, the Tezos blockchain project raised $232 million and represented the largest fundraising effort

The Tezos blockchain project raised

$232 million

and represented the largest fundraising effort by a blockchain-based company strictly through a token sale

by a blockchain-based company strictly through a token sale as of January 2018. [333] 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. [334] 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 presale and $48 million in public sale), $27 million short of their goal.[335]

ICOs experienced a significant increase in the dollar amount of funding until June 2018, with start-ups doubling the amount of funding raised in 2017 in the first half of 2018 alone. In June 2018, EOS, a start-up focused on smart contract technology, raised a record $4.1 billion in funding through its ICO, which became the largest fundraising effort through an ICO to date. The market for ICO funding fell back to 2017 levels in the month of July. [336]

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, [337] it's easy to see why a cheaper and potentially less regulated method for fundraising is desired. That being said, the uncertainty regarding the 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 nearly $220 billion, [338] up from just under $20 billion at the beginning of 2017. The price of bitcoin stabilized in the latter half of 2018, and with that, the cryptocurrency market has seen an influx of hedge fund and institutional investor investment. This activity has spurred more over-the-counter cryptocurrency purchases and the establishment of brokerage firms to help institutional buyers find the inventory they need. [339] According to the hedge fund analysis firm Eurekahedge, from June 2013 through April 2017, the Eurekahedge Crypto-Currency Fund Index returned a cumulative of 2,152.42 percent. [340] On an annualized basis, this comes to 125.45 percent for actively managed digital asset strategies, outperforming the Bitcoin Price Index by 103 percent. [341]

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.

SEC

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 presales or currency sales, rather than public equity offerings, in a misguided attempt to escape regulatory burdens associated with securities. The SEC has jurisdiction over "securities," as defined in Section 21(a) of the Securities Act and Section 3(a)(1) of the Exchange Act. [342] The term "security" includes, among other things, "investment contracts." "Investment contract" is a prophylactic catchall term that captures atypical products that function as devices for raising money. [343] 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. [344] 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. [345]

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) offered through the Ethereum network constituted an offering of securities. [346] The SEC explained that "U.S. federal securities law may apply to various activities, including DLT, 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." [347] 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 derived from 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.

In June 2018, the Director of the Division of Corporate Finance at the SEC, William Hinman, stated at the Yahoo Finance All Markets Summit: Crypto, that it is possible for digital tokens issued in ICOs not to be considered to represent securities offerings even after they were considered to represent securities when initially issued. Hinman stated, "if the network on which the token or coin is to function is sufficiently decentralized – where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts – the assets may not represent an investment contract." [348] In other words, Hinman's statement explains that it is the SEC's view that the circumstances surrounding a digital asset and the manner in which it is sold is the focus for making a securities classification determination, not the digital asset itself. At the same conference, Hinman put forth bitcoin and ether as two examples of tokens without a central third party whose efforts are a key determining factor in the enterprise, whose offer and sale are not securities transactions, effectively ruling that bitcoin and ether were both properly classified as commodities and not securities.

CFTC

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. [349] 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."

Other Considerations

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 (POC) before the token sale. From a potential investor's perspective, the lack of a POC 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 (for example, 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, AML 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 have also begun to provide some clarity about the regulatory treatment of token sales. The 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. [350] Similarly, on September 9, 2017, the UK FCA 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. [351] Hong Kong's financial regulator, the 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. [352] In June 2017, the chairman of the Australian Securities Investment Commission 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 they have the same characteristics.[353] 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. [354] 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). [355] More recently, Quebec's regulator for financial institutions, the AMF, determined that a token offered by Impak Finance was a security, but accepted the company into its regulatory sandbox,

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

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. [356]

In stark contrast to the actions of Canada, as discussed in the chapters on international regulatory landscape, China officially outlawed token sales on September 4, 2017, requiring all persons and organizations that had previously completed token sales to refund their investors. [357] 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, 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 and 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. [358] 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.[359] The Ethereum blockchain underwent three subsequent hard forks to resolve security issues that gave way to malicious network attacks. [360] While each hard fork was intended to resolve existing scaling and security issues, future hard 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 increasingly more 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, how 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 increased 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 developments the future will bring.

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

Chapter 11 **Blockchain innovation in energy, commodities, shipping, and trade finance**

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

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

At first glance, the convergence of the antiquated and long-established world [361] 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 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. [362]

The Natixis-, IBM-, and Trafigura-pioneered DLT crude oil trading platform is an excellent example of this, [363] 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-to-peer energy trading. The well-known example of Brooklyn's solar microgrid, [364] 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 POC 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 high level, an autonomous distributed ledger in which transactions are executed directly between producers and consumers has the potential to decentralize the often-rigid energy ecosystem and increase transparency and efficiency, empowering end users in the process.

Peer-to-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. [365]

Of course, many of the complex and intricate regulations that underpin national power markets, for example, the UK's Balancing and Settlement Code, [366] 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 consumer 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, [367] 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 published data that shows that the average gas and electric switching time in the UK is 16 days. 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 begun a consultation phase on plans to deliver next-day switching across the country by 2021. [369] 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 may very well help OFGEM (and similar national bodies) to achieve this goal. For example, in March 2019, Electron, an Ethereum blockchain-based decentralized meter registration platform, partnered with the National Grid and SP Energy Networks to develop a platform that facilitates the sharing of energy asset data, called RecorDER. The use of blockchain technology eliminates the need for a central party-hosted system that would require considerable infrastructure. Regulators like OFGEM can work with these companies to generate shared datasets for regulation too.[370]

Taking this one step further, smart contract code may 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, and producers to their respective assets, simplifying the multilayered 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 obligations imposed by certain legislation, such as the European powers and gas regulation, REMIT. [371]

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. For example, VOLTEX (a company deploying blockchain-based energy management) integrated smart contracts into their blockchain platform that allow for electricity to be traded automatically. [372] 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. This is one of the issues currently precluding the development of blockchain-based solutions that can handle higher-voltage energy trades. [373]

Research into smaller scale, peer-to-peer trades is currently more prevalent. Shell Ventures and Sumitomo Corporation Group both recently invested in LO3 Energy, which are developing a blockchain platform for peer-to-peer energy trading. [374] This kind of energy trade is in its nascent stages, with machine learning company Verv facilitating the first peer-to-peer energy trade in the UK in April 2019. [375]

Further, the potential removal of a central entity 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 and implementation of certain conditional logic triggers for these eventualities [376] 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.

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 markets for these products highly liquid in the future. Energy derivative transactions may also 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. [377] 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. One bilur energy token is equivalent to 1 ton oil equivalent of Brent crude or 6.481 barrels. One bilur gold token is equivalent to one troy ounce of gold. It is issued on a private Ethereum network and may be traded among individuals or on an organized digital asset exchange.

As this market develops, these products are becoming more innovative and complicated. For example, the Swiss asset manager and commodities trader Tiberius Group launched Tiberius Coin in late 2018. [378] The token is backed by a basket of seven metals ranging from copper to cobalt that Tiberius Group believe are "key to future technologies."

Energy trading platforms

In the future, energy products may be traded on decentralized order books that rely 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. [379] The platform would offer day-ahead, monthly, quarterly, and yearly baseload for power and gas. The project successfully completed its POC phase and went live on 20 May 2019. [380]

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. [381] Notably, Sharing Energy Co. (a Japanese solar energy installer and provider) joined forces with Power Ledger (an Australian blockchain start-up) to enable the sale of energy on its platform. While the project will initially be limited to the sharing of real-time usage data from smart-meters, this data will eventually be used to support energy trades between buyers and sellers using the blockchain. [382]

Physical energy transactions

Companies are developing blockchain technologies to streamline physical commodity transactions. In February 2018, commodity trading house Mercuria and the banks ING and Société Générale executed a large oil transaction using a blockchain platform called Easy Trading Connect. The parties found that the technology reduced the amount of paperwork required for title to pass from buyer to shipper to seller. African crude was bought and sold three times in transit on its way to China, with the average time for a bank to perform their role in the transaction falling from three hours to just 25 minutes. The distributed ledger also minimized the risk of documentary fraud. [383]

Commodity trading firm Trafigura and French bank Natixis are two of a group of 15 institutions aiming to "digitalise the trade and commodities finance sector through […] blockchain," [384] collectively forming komgo SA. [385] 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. Two successful (Ethereum-based) POCs have been developed: Easy Trading Connect 1 and 2, which standardize and expedite KYC requests and issue digital letters of credit respectively. [386]

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.

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. [387] 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 the 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.

For more information, please read the smart contracts chapter in this white paper.

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, [388] 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. [389] 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. [390] 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. [391] 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. [392]

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 IoT to achieve real-time monitoring and managing of reefer containers during the pilot voyage. [393]

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. [394] 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, and ocean carriers, customs authorities, and other relevant parties the ability to access a complete set of constantly updating documents. It would also, 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

Electronic bills of lading (e-bills) are not a new concept. [395] 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 ETSs 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 life cycle, e-bills created on centralized ETS such as Bolero are equally vulnerable to cyberattacks, a threat that is not covered by P&I coverage. Blockchain mitigates this risk by decentralizing the system and making it significantly harder to hack. Indeed, in the wake of a 2017 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. [396]

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.[397] The platform, in which went live in May 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. [398]

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. [399] 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." [400] 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. [401] 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 preset conditions, rather than upon the counterparty's notice of satisfaction of those conditions), the self-executing nature of smart contracts reduces the risk of noncompliance. 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. [402] 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 they 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. [403] Please see the chapter on smart contracts 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.

Aviation

There have been some forays into the world of blockchain by the aviation community, however, the fintech impact in the world of aircraft leasing and finance has so far been less pronounced than some others. Airlines such as AirBaltic in Latvia and Peach in Japan have accepted payments made in a virtual currency. According to the Financial Times in May 2018, International Airlines Group (IAG) is of the view that blockchain is a "key priority," and Lufthansa has started a "blockchain for aviation" initiative. However, selling airfares or cataloging passenger preferences is some distance from settling aircraft sale and purchase transactions through this medium – and it offers appreciably less value as well.

We do see there potentially being numerous applications of blockchain technology across the aviation sector. A huge amount of data is produced by, and required for, every aircraft-related transaction – from the sale and purchase of the aircraft, its management and maintenance, its operation, and its leasing. With this in mind, we will take a look at some of the potential uses for, and benefits of, blockchain technology in the aircraft leasing and financing industry.

1) Sale and purchase

In our view, it is feasible for participants in aircraft sale and purchase transactions to establish a blockchain-based trading platform for the sale and purchase of aircraft. Aircraft sale and purchase transactions could be concluded on the basis of smart contracts. This would be effected by "tokenizing" the asset. This token could then be traded in exchange for payment in a virtual currency.

As noted above, virtual currencies are already being used for airline ticketing, but this is still some way from reaching the level of acceptance required to be used to finance the sale and purchase of an aircraft. However, there are anecdotal examples of large asset transactions already being closed using Bitcoin, especially in the real estate sector.

The sale of an aircraft could also be automatically effected at a time and in a location by the relevant blockchain to minimize sales or transfer taxes, only releasing the relevant "signatures" (whether digital or otherwise) to smart contracts or other digital title transfer documents at the time when the aircraft or an oracle automatically confirms to the relevant blockchain that it is in a suitable jurisdiction.

In addition, the value of a used aircraft is of course in no small measure contingent on its condition and its maintenance history. A purchaser will need to be comfortable that the aircraft's history has been properly and completely documented and those records will need to be made available to the purchaser in a way that it can rely on them. Blockchain could be used to provide an instant and practically incorruptible record of parts fitted to an aircraft and the integrity of their maintenance. It could in theory be as instant and simple as scanning a barcode on the side of an engine with a smart phone, revealing that engine's comprehensive history.

This would greatly facilitate technical due diligence (and increase the accuracy of that due diligence), speeding up sale and purchase transactions by making the evaluation of each asset more straightforward. In this scenario, it should not matter how many previous owners an aircraft has had – it would still be possible to identify the age and provenance of each part. The increased efficiency of blockchain in this area could offer significant time and cost savings, and it would likely also contribute to the industry's safety.

2) Financing

We recognize this may still seem far-fetched, but we do not think the day that aviation financiers lend in a virtual currency is far away. The ability to purchase an aircraft with a virtual currency will be inextricably linked to the ability to raise finance in virtual currencies. However, pricing virtual debt is difficult. Further, aircraft are, of course, capital intensive, and there is a relatively low level of virtual liquidity. Virtual currencies are also somewhat volatile when compared to traditional currencies. The first movers are therefore likely to be the leading manufacturers, for whom a key advantage will be the ability to peg the purchase price for a new aircraft to their airline customer's "real" domestic currency, thus mitigating any foreign exchange exposure.

Foreign exchange risk is also a particular issue for airlines who often raise finance (and pay lease rentals) in U.S. dollars but generate their income in a "home" currency. Using virtual currencies to meet these payments would enable greater foreign exchange mitigation for them as well.

Notwithstanding the issues that remain to be resolved around virtual debt, it strikes us that while statistically most aircraft are financed by bank debt (and we anticipate that this will continue to be the leading source of funding), it is systemically not the best option for either lenders or borrowers. Existing methods of financing aircraft are document heavy and rely on negotiating provisions that could and arguably should be harmonized to all parties' benefit. There is a necessary level of rigor and bureaucracy from all participants that, although important, could perhaps be better accomplished through greater automation in a blockchain environment. Smart contracts, for example, could greatly streamline transaction management and the execution of significant numbers of transaction documents, even if bespoke provisions still remained to be negotiated.

Further, security interests and their relative priority vis-à-vis other interests could also be recorded as an immutable and transnational public record of the interests of each owner and investor or financier in an aircraft – as well as providing the ability for liens of third parties to be publically recorded if and when they arise. All of this could be used in conjunction with existing public databases and, in particular, the International Registry operated pursuant to the Cape Town Convention.

3) Aircraft leasing, management, and maintenance

Because of the relative duration of the aircraft lifespan and the frequency with which critical component parts are replaced, we are of the view that maintenance databases maintained by airlines, aircraft operators, and maintenance facilities would be ideally suited to management in a blockchain environment, giving greater levels of traceability and trust. This in turn would serve to increase the liquidity available to the industry.

All of the millions of component parts of aircraft are managed by different and often uncoordinated systems. These records may be incomplete, and some are still paper-based. This lack of standardization leads to challenges in traceability and compliance. It would in our view be more efficient if all relevant stakeholders submitted transaction details to a private blockchain established by, for example, a manufacturer. Every action in relation to the component parts of an aircraft throughout its lifespan could then be recorded, timestamped and would be able to be relied upon. This would benefit the manufacturers, MROs, lessors, and airlines alike.

Much of the underlying infrastructure already exists. In particular, each major component part of an aircraft will already have a unique identifying serial number; and a lot of work has been done to establish digitized databases. However, not only is there a lack of standardization, but these databases are heavily reliant on input by human operators. By its nature, any database with inputs provided by a human is subject to the risk of both fraudulent and negligent misstatement – a risk that is mitigated by blockchain. Our expectation is that it could be automated such that the requirement for manual data entry is minimized, which would be particularly valuable for engines. However, there is a need for an industry-wide consensus to be reached for this to succeed – the majority of market participants would need to join a common platform to realize the value and potential in such a system.

Implementing a blockchain system could also be used to track the use of the individual aircraft (for example, take-offs and landings, flight hours, engine cycles, etc.), which could identify when replacement or maintenance is required. These inputs would yield real-time outputs and improved data quality. More than just tracking the replacement or maintenance of parts, a blockchain could also be used to take data directly from the aircraft's sensors

and record the occurrence of damage events leading to the replacement of parts (or, at least, the requirement to do so).

To make this work, data ownership and privacy issues will need to be resolved, as will security concerns – both commercial and operational. Each component supplier in addition to the airframe and engine manufacturer would ideally have the ability to input in the record as appropriate. Payment for the replacement or service of parts could also be automated through the system. However, we anticipate that principally because of the cost and "unknowns" that inevitably have to be borne by first adopters, any approach is likely to be driven initially by the principal airframe and engine manufacturers and will then evolve over time to become more comprehensive.

Further, as noted above in the context of sale and purchase transactions, our view is that leasing transactions could helpfully be concluded on the basis of smart contracts. This could include the use of ancillary chains to the primary blockchain, enabling each individual aircraft asset to be given its own ancillary chain. This would provide greater opportunity for analysis at a fleet level, as well as a more granular asset level.

We anticipate that lessors adopting blockchain technology first will gain a competitive advantage because their business will be able to run more efficiently. It may also mean that they can attract investment from a wider variety of funding sources who will be attracted by the accurate, timely, and comprehensive reporting – especially where those investors may not be native English speakers. If English was the language of the industrial revolution, code is the new language of the cyber revolution.

4) Documentation

The merits of smart contracts have been discussed earlier in this paper.

In particular, blockchain would provide a platform for transaction documents of any nature to be stored on a single, immutable, and shareable database. This would help mitigate against fraud and would enable largely paperless and totally accurate transactions, free of human error. Even if certain paper documents are still required, transacting by blockchain would greatly assist with the processing and (where applicable) transfer of any originals. For example, parties may be able to dispense with the need for multiple duplicate documents, whether in original "hard copy" format or indeed soft (electronic) copies on other databases.

Blockchain transactions would provide for all transaction details to be logged and stored free from documentary fraud and visible to all applicable stakeholders, replacing systems that are susceptible to both forgeries and simple clerical errors.

a) Aircraft insurance

In the insurance space, it is necessary to ensure in particular that appropriate liability policies are in place – not just at the outset of the transaction but on an ongoing basis. Renewals could be effected automatically within a blockchain and the appropriate parties (lessors and lenders as well as airlines) would be informed that this had happened. This removes the risk for a lessor or lender of failing to notice that a renewal has not happened. It also reduces the need for active diarizing and monitoring by individual employees who may leave or be away from the office at the crucial time of renewal.

b) Title registration and bills of sale

Establishing title to an asset is paramount – especially in the event that it is sold. Much time is spent and cost incurred in storing and cataloging and then retrieving and delivering each bill of sale from each transaction to which that aircraft has been subject from its initial delivery by the manufacturer. Many readers will be only too familiar with the scenario of missing original bills of sale and the need for sellers to provide additional title warranties as a consequence.

We are of the view that any global blockchain registry or title database is an unlikely innovation because of the level of change this would require to underlying legal frameworks. However, a distributed ledger means that the ownership of any particular digital asset is much more certain, making its identification more akin to a property title search. This could therefore serve to replace the need for paper bills of sale. Blockchain offers a particular advantage in this regard as its integrity and resistance to fraud are ideally suited to such uses.

Various stakeholders in other industries have already explored similar capabilities, particularly in the world of real estate. The Swedish land registry has been trialing blockchain-based solutions since 2016. Their research has apparently indicated

that eliminating paperwork could save taxpayers millions of euros every year and reports suggest that a test transaction is imminent. In other examples, Amaravati, a city in India, created a land registry based on blockchain, and Dubai decided to migrate its land registry to a real estate blockchain – including for lease transactions. Dubai has also gone one stage further, aiming to link its real estate registrations with its public utility provisions thus ensuring that all property-related accounts are settled immediately and automatically. These states are not alone in taking the plunge.

Legal obstacles, such as the validity of digital signatures, will need to be resolved and any progress will not work in technological or jurisdictional isolation – needing significant international consensus akin to (if not greater than) that achieved with the Cape Town Convention.

c) Letter of credit

As discussed earlier in this paper, there are a number of immediate applications in this regard and a blockchain-based letter of credit would be just as useful in aviation as it would in the world of trade finance.

5) Conclusions

This review is by no means exhaustive, but there is enough to indicate that the characteristics of the airline industry align very well with the capabilities of blockchain. We note also that there are many other applications of blockchain in particular that are outside the scope of this paper, such as:

- Passenger services, like paperless ticketing;
- Flight planning (air traffic control and the associated flight charges, for example, Eurocontrol); and
- Loyalty programs.

It will take time for law and market practice around blockchain and smart contracts to become clear and capable of reliance, but the application of blockchain will eventually go far beyond our current expectations for it.

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 has been largely paper-based, expensive, and complicated for decades, and appears to be long overdue – and the key players in the market together with potential participants are all welcoming to the change.

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 DLT. [404] 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.

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. Since around five 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. [405] Blockchain is updated quickly by each member on the network and shows the most recent transactions, so 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 recognized as a reliable way to stop documentary fraud 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.[406] 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.

In a report prepared by Bain & Company, a global management consultancy, it was estimated that blockchain could increase global trade volumes by $1.1 trillion by 2026, from the current base of $16 trillion. [407]

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.

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

The seven steps to a typical 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. [408]

One of the most prominent initiatives relating to letter of credit transactions is Voltron, which is built by CryptoBLK on R3's Corda framework and run by a consortium of eight founding members: Bangkok Bank, BNP Paribas, CTBC Holding, HSBC, ING, NatWest, SEB, and Standard Chartered. In May 2019, it was reported that 50 banks and corporates have joined the project to carry out a six-week trial. The members have also completed five "live" commercial pilots in different locations; the application has so far demonstrated significant improvement in transaction speed, reducing the time it takes to execute the entire process of a paper-based letter of credit from five to 10 days, to under 24 hours. Compared to earlier trials, which were mostly focused on testing the technology and markets, this new project is predominantly about scale. [409]

A different solution was presented by the founders of Singapore-based invoice finance provider Incomlend, who are launching LC Lite – a blockchain-based platform which would remove the need for the exporter and importer banks, allowing the parties to issue, amend, track, and execute letters of credit. It is intended that the banks will still provide the credit or guarantee to the importer, but the letter of credit management will be performed via the LC Lite platform. [410]

Latest commercial developments

In the last few years a number of new platforms have emerged, prompting the market to consolidate. Some commentators have noted that corporates and banks sometimes revert to using a particular platform in a particular region, faced with the difficulty of differentiating between the available platforms. [411]

In October 2018, blockchain platforms We.trade and Batavia announced that they would merge. Both were built by IBM, based on the Hyperledger Fabric blockchain framework and sought to digitize open account trade finance. As of March 2019, 14 major European banks – including CaixaBank, Deutsche Bank, Erste Group, HSBC, KBC, Natixis, Nordea, Rabobank, Santander, Société Générale, UBS, and UniCredit banks – have signed licenses to use it. IBM claims that we.trade and its member banks are "opening the door to trade finance for 70 percent of small and mid-sized business in Europe that previously did not have access." [412]

Drawing on their experience to date, industry specialists have noted that to realize the true potential of blockchain, platform developers and participant entities will need to avoid fragmentation that limits the wider adoption of the technology. In this context, the banks, in particular, will have to agree on acceptable standards and business processes. At the same time, some industry commentators see a need for "superconnectors" – trusted institutions such as large banks that connect various existing networks. [413]

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. It would become an even bigger issue if the market moves toward using open ledgers, which involve indirect participants such as warehousing companies, end buyers, and insurers.

Legal enforceability of smart contracts is another concern, as we analyze in the section above. Some 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.

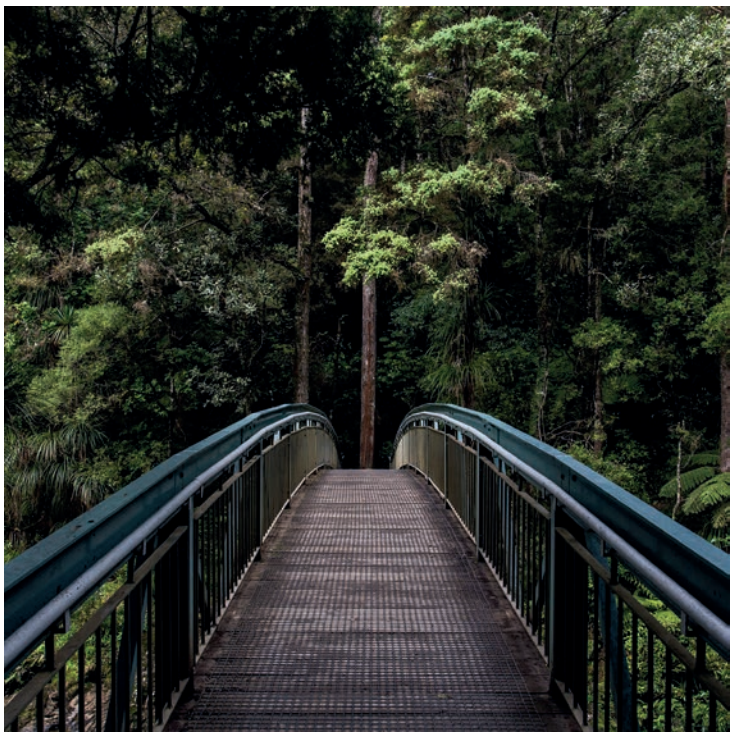
Sanctions

We have seen that some of the most used platforms on the market are U.S.-owned and, as a result, the U.S. sanctions would be considered in particular. If blockchain technology is owned or developed in the United States or by U.S. persons, it is likely to be subject to U.S. jurisdiction and may also be subject to U.S. export controls depending on the technology used. This causes a problem to the developers as it means that even if default rules of the system allow certain transactions (for example, an Iran-related trade financing involving non-U.S. entities), its design should provide for prevention of such transactions. Building in such mechanism could prove to be rather challenging considering that certain regulators can impose new sanctions without notice. As a result, the developers need to consider a number of factors such as the place of development of technology and from which places it can be accessed, and potentially restricting access from sanctioned locations.

In a wider sanctions context, other risks relate to failure to enter relevant or accurate information into the ledger (for example, details of the importer and exporter, the banks involved, and the ports of loading/discharge). To avoid any issues, it could be advisable for the parties to agree to the precise date that needs to be input into the system and which party is responsible for it.

Confidentiality

The transparency of the blockchain can be difficult to reconcile with the privacy requirements of the banks and other parties – once the information is added to the ledger, it is not easy to have it removed. Another concern for the banks is that some of the information that may be required to be disclosed on the blockchain system may be prohibited from disclosure by law



Chapter 12 **Privacy and re-identification on the blockchain**

As one paper noted, "anonymous digital cash is another state-of-the-art technology for Internet privacy…many observers have stressed [that] 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..." [414] When the paper in question, "Privacy-enhancing technologies for the Internet" was published in 1997, its authors were thinking not of Bitcoin but of its predecessor, DigiCash's "Ecash." However, in the 20 years since, the risks to privacy and anonymity identified in the paper 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. [415]

In blockchain technology, and its early co-emergent currency products such as bitcoin and ether, the wildest dreams of DigiCash's founders have been realized: there now exists not one but dozens of truly anonymous networks facilitating commercial transactions on a global scale. But so too have their fears. As the web of virtual connections grows ever more dense and tangled, and the analytic power being applied to it increases with exponential regularity, even the most secure blockchain protocols will pose a very real risk of re-identification; and certain digital ledgers actually provide more anonymity than any previous form of transactional records. [416]

Anonymity versus privacy

Today, the predominant blockchain protocols, following the model of Bitcoin, have 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 blockchain."[417] In addition, an individual user may use one (or more) public keys (sometimes referred to as addresses) to engage in transactions on the blockchain, further anonymizing their activities. These public keys do not identify individual users, and without additional data or analysis, it cannot be determined whether two (or more) public keys are linked to the same user. Yet at the same time, the transactions exist in public for anyone to see. Therefore, the Bitcoin protocol provides for anonymity, but not privacy. The danger of Bitcoin (and similarly constructed protocols) is that with sufficient analytic power, or insufficient care from users, the ledger of public, anonymized transactions can be reverse engineered to allow an interested party to determine the private identities lurking behind, often through relatively unsophisticated means, like the use of web trackers and cookies leaked by merchants that transact in Bitcoin. [418]

These dangers belie part of the purpose for which Bitcoin was founded. In the wake of major breaches of traditional, centralized databases containing personally identifiable information (PII), pioneers of blockchain technology have argued that decentralized networks are more capable of protecting privacy in the long run, by giving more agency over PII to individuals and preventing the risky accumulation of data in the first place. Redistributing 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. [419]

However, as the inventors of Ecash warned more than 20 years ago, a chain is only as strong as its weakest link. In the short term, numerous "off-ramps," such as crypto exchanges, virtual wallets, and IP addresses all pose extrinsic risks of re-identification for anonymous users, while the application of "big data" can pose an intrinsic risk to the protocols themselves. In practice, the much-touted anonymity of any blockchain is dependent on a grid

of pseudonymous and identity-laden infrastructure. Without taking adequate precautions, user data may actually be less secure than if it were stored in a more traditional, centralized manner.

Re-identification risks on the blockchain

Risks to PII on the blockchain take two primary forms: extrinsic risks, such as Bitcoin wallets, virtual currency exchanges, and private data breaches, and intrinsic risks posed by analysis of the blockchain itself. Of the two, the extrinsic risks are easier to comprehend and mitigate; while the intrinsic risks pose difficult, perhaps even fundamental, questions to the interpretation and practice of privacy law.

The paradigmatic example of an extrinsic risk is a user purchasing digital currency through an online wallet or currency exchange. In order to complete the transaction, that wallet or exchange service must be given the personal information of the purchaser (nothing short of a Social Security number for purchasers inside the United States). 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.

Similarly, some users voluntarily reveal their public keys, whether publicly (as may be the case for businesses accepting digital currencies as payment) or through "phone-book" style search engines such as that hosted by blockchain.info. Still others disclose this data in more private settings, such as forums, emails, messages, or signature lines. In this respect, one may think of a blockchain application's public key as 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), while others may voluntarily disclose some or all of that personal data in exchange for increased publicity and, with it, functionality.

Another category of users will divulge sensitive personal information accidentally while transacting anonymously. Those who are able to link public keys with this outside identifying information may then have the ability to analyze the blockchain and 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.

The GDPR takes a similar approach in respect of its definition of personal data but does not take it quite as far as the mere knowledge of a purchase being made. An individual is required to be identified or identifiable by carrying out further research (such as via a search engine) in order for that definition to be satisfied. "Online identifiers," such as IP addresses and location data are specifically included as, in a crude sense, they give third parties the ability to make contact with the individual concerned.

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. As above, digital currencies for these users are effectively no more anonymous than a bank account.

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."[420] 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 website'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. [421]

Finally, there are the intrinsic risks. Unlike the risks discussed so far, which all in some way circumvent the basic anonymizing principle of the blockchain, intrinsic risk is created by the structure of the blockchain itself. The process of recording and managing sensitive information on blockchains poses unique challenges, 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. [422] Such large data sets contain an inherent asymmetry: while they may be inaccessibly large to any human mind, a sufficiently strong computer could look for patterns that a human would find undiscernible. [423]

Of course, every form of extensive activity is potentially subject to re-identification. This theoretically includes activity on the blockchain, [424] and, in fact, researchers and law enforcement agencies have already been able to re-identify bitcoin activity, through the application of "transaction graph analysis" to identify bitcoin merchants and customers; and have applied similar methodologies to smart contract operations.

Some developers have tried adding additional layers of privacy to design around the availability of participant and transaction information on the blockchain via "privacy coins." 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.[425] Monero is another example of a blockchain-based network that obfuscates digital currency data including transaction sources and amounts through advanced cryptography, transaction-specific, one-time addresses, and obfuscated signatures.[426] While these approaches can help prevent re-identification, masking network participants also makes it more difficult for legitimate businesses to make use of the protocol and frustrates the ability of AML measures to identify illegal transactions. [427]

Pseudonymity as a model

Some of the concerns surrounding privacy on the blockchain are similar to those raised when discussing pseudonymity in other industries and contexts. For example, the National Institute for Standards and Technology (NIST) has issued standards regarding pseudonymity and de-identification. In a recent report, the NIST defines pseudonymization as a "specific kind of de-identification in which the direct identifiers [like names or account numbers] are replaced with pseudonyms."[428] 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."[429] 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." [430]

masking network participants also makes it more difficult for legitimate businesses to make use of the protocol and frustrates the ability of AML measures to identify illegal transactions

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.[431] 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."[432] In the case of DLT, 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. Absent some countervailing tendency, the result will be an ever-increasing risk of re-identification.

In this sense, a blockchain can be thought of as a certain kind of pseudonymized data set, where PII such as name and location is replaced with a virtual address. Looked at from this perspective, the NIST standards are largely meant to provide uniformity in the pseudonymization of data sets, to help companies not inadvertently reveal sensitive client information. Standards of pseudonymity on the blockchain, by contrast, are more well-known and, in fact, often spelled out explicitly in the protocol. Further, blockchain users have more control over exactly what data they exchange, and they can take various actions to maintain greater privacy (however, this increased privacy may come at the cost of higher transaction fees).

By allowing for identifiability, pseudonymized personal data "stays inside the scope of the legal regime of data protection."[433] 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.[434] 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." [435]

Pseudonymization is a key concern to big data generally, and is at the forefront of the minds of actors in a number of industries currently grappling with the potential for blockchain to revolutionize the privacy risks inherent in such high levels of transparency. NIST's concern regarding re-identification risk is mirrored internationally as described below.

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 because "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." [436] 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[437] 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. [438]

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. However, 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.[439] 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 both in and out of the financial services context.

Smart contracts

As elaborated elsewhere in this white paper, 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 they 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.[440] 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" above 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." [441] 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. [442]

Pseudonymity is also a "double-edged sword" when it comes to smart contracts, as the ability to obfuscate a party's identity might yield greater privacy protections in certain contexts, but the less information available about a counterparty to a smart contract, the more difficult it will be to practically enforce or seek recourse for any errors that occur outside of the smart contract's protocol.

Compatibility with regulation

The GDPR requires "appropriate organizational and technical measures to ensure a level of security appropriate to the risk" in respect of the handling of any personal data. It suggests, only as examples, the use of anonymization and encryption techniques to meet this security requirement. Use of these techniques will depend on the nature, scope, context, and purpose of the personal data handling, and the risks posed to the individuals concerned.

The decentralized nature of blockchain technology is often considered to be incompatible with the GDPR. By requiring organizations as "controllers" to handle information relating to an identified or identifiable individual (known as personal data) according to a prescribed set of principles, the GDPR aims to ensure the protection of the fundamental rights and freedoms of individuals, including the right to privacy. However, the decentralizing principle of a blockchain network means that all its members hold the same records (including relating to individuals) and contribute equally to the stability of the network. This could create serious GDPR compliance issues in the event that any part of the network, or the service it provides, has an EU element to it. The homogeneity of the blockchain network would mean that all of its members are considered to be controllers who are subject to the GDPR regardless of their location. Those controllers would have direct responsibility under the GDPR and would thus be required to put in place contractual arrangements between them governing the sharing of personal data and the creation of appropriate safeguards to prevent its misuse. Were such a network containing personal data to be public and permission-less – as is the case with most existing blockchain protocols – the issues over compliance only deepen.

The French data supervisory authority published some guidance that generally confirms the understanding that although prima facie technology is neutral, the model of data processing envisaged by the GDPR is not compatible in many ways with blockchain. In particular, the immutability of data recorded on the blockchain would make complying with storage limitation principles and effecting a data user's request to rectify data difficult. The supervisory authority suggests that alternate technical solutions could be used to achieve effectively the same result. In the case of storage limitation or exercise of a right to be forgotten by a user, deletion of the relevant private key from the hash function would effectively make the data inaccessible. Incorrect data can be remedied with the inclusion of correct data into a new block of a later transaction superseding the original incorrect data. Similarly, the high number of controllers in a blockchain relationship has been recognized as a key obstacle to compliance. Guidance from the supervisory authority suggests that controllers designate an agent party to act on their behalf as a class. These remain suggestions from just one European data supervisory authority, and although correct at the time of publication, we expect swift regulatory development in this area.

Similarly, the California Consumer Privacy Act provides consumers with a right to erasure of their personal information.[443] Such a right could problematize the use of a de-centralized network and the immutability of a digital ledger that holds permanent data storage as a fundamental feature. While permanent and unchangeable storage has its benefits from a recordkeeping perspective, current and future regulation may lack the flexibility needed to ensure the technology's compliance from a privacy perspective.

As well as privacy laws, blockchain in the form of cryptocurrency has come under increasing regulatory attention from financial and prudential regulators – especially in Europe. The UK regulator, the FCA, proposed a ban on retail investors dealing in derivatives where cryptocurrencies such as bitcoin make up the underlying asset. In the notice setting out the proposed ban, the FCA cited volatility and issues with valuation as features that might cause retail clients to suffer sudden and unexpected losses. The FCA also identified information asymmetries as a key area of concern around retail investors' ability to make well-informed decisions. Other areas of concern highlighted by the regulator include cyber risk, financial crime, and market abuse.

Conclusion

Today, the world is closer than ever to operating on a truly anonymous and private global transactional network. However, its realization is prevented by problems both old and new. On the one hand, all the vulnerabilities that existed in the days of Ecash still exist today: entry points with "trusted" centralized databases, IP traffic subject to panoptic scrutiny, the constraints of functionality, theft, and user error. To this long list has been added the more recent concern posed by the exponentially improving analytic capabilities of big data and artificial intelligence, which together threaten to overwhelm the pseudonymity of any sufficiently large data set.

Ultimately, while the risk of re-identification cannot be wholly avoided, it can be mitigated through vigilance and good practices. Those using Bitcoins and DLT should be aware of the already-identified risks inherent in the current model and take steps to reduce such risks by incorporating encryption or obfuscation into their blockchains and into their personal transacting habits.

Blockchains were not originally conceived with identity management and privacy in mind.

Chapter 13 **Intellectual property**

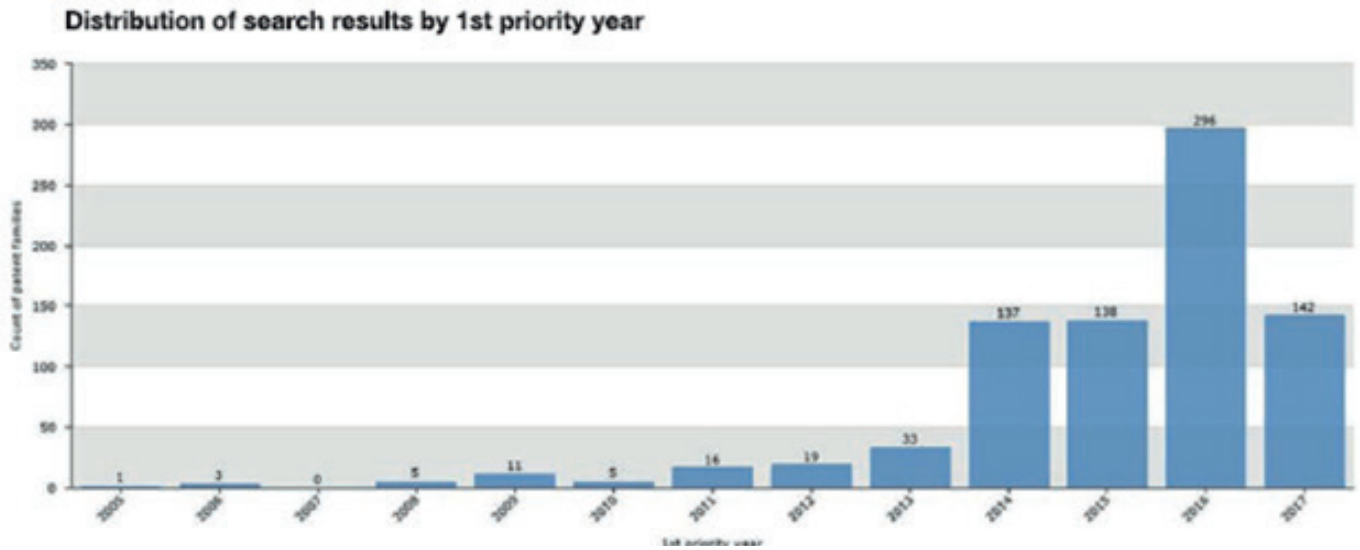
While Bitcoin made the blockchain famous, the benefits of a secure distributed ledger are being implemented across many fields. Ancillary technologies are being invented to improve and expand digital currency services, improve block mining, and utilize distributed ledger technologies in new ways. As 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 License that allows others to freely use, modify, and share the software.[444] Other digital currency and distributed ledger projects are similarly distributed under open-source licenses, but the licenses vary. For example, Ethereum applications are distributed under the GNU General Public License, but the core engine of Ethereum is under a more liberal license.[445] Litecoin is released under the MIT License.[446] And OpenChain is released under the Apache License.[447] 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.[448] The MIT License grants any person with a copy of the licensed software the rights to use, 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. Bitcoin 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 need to be aware of the terms of the license to the specific software they are using to understand their rights and potential liabilities. Likewise, companies developing new blockchain technologies will want to ensure they are taking appropriate steps to protect their own innovations while adhering to existing license requirements.



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. One of its stated missions 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. [449]

While the Hyperledger Project is open source, its open-source license is different from the MIT License under which the Bitcoin software is distributed. Inbound code contributions to the Hyperledger Project must be made under, and outbound code will be made available under, the Apache License, Version 2.0 (V2.0).[450] 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 need to be aware of the specific open-source licenses governing the blockchain-related technologies they are using. The terms of these licenses may impose obligations beyond those of the MIT or Apache licenses, such as a requirement to make available the object or source code for modified versions of the licensed works. Companies using or developing blockchain technologies that are unaware of the specific terms of relevant licenses risk liability.

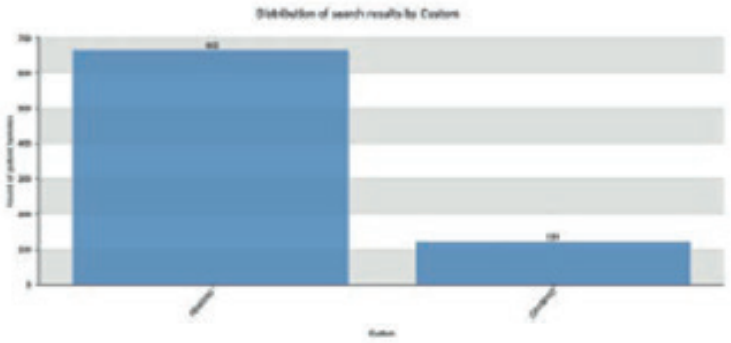
The rise of blockchain patents

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 chart above shows the number of new patent applications (by family) directed specifically to blockchain technologies filed per year from 2005 through 2018 on the horizontal axis.[451] As shown, there were almost seven times as many new patent filings in 2017 as there were in 2014. Patent applications can take 18 months to publish, so the data for 2017 and 2018 remains incomplete. As more applications publish, we expect to find an even sharper rise. Cryptocurrencies and the underlying DLT inherently reach across borders. Patent application filings provide an indication of anticipated markets for developing technology. The map on the following page shows individual patent filings in each country, with darker blue indicating a greater number of filings. [452]

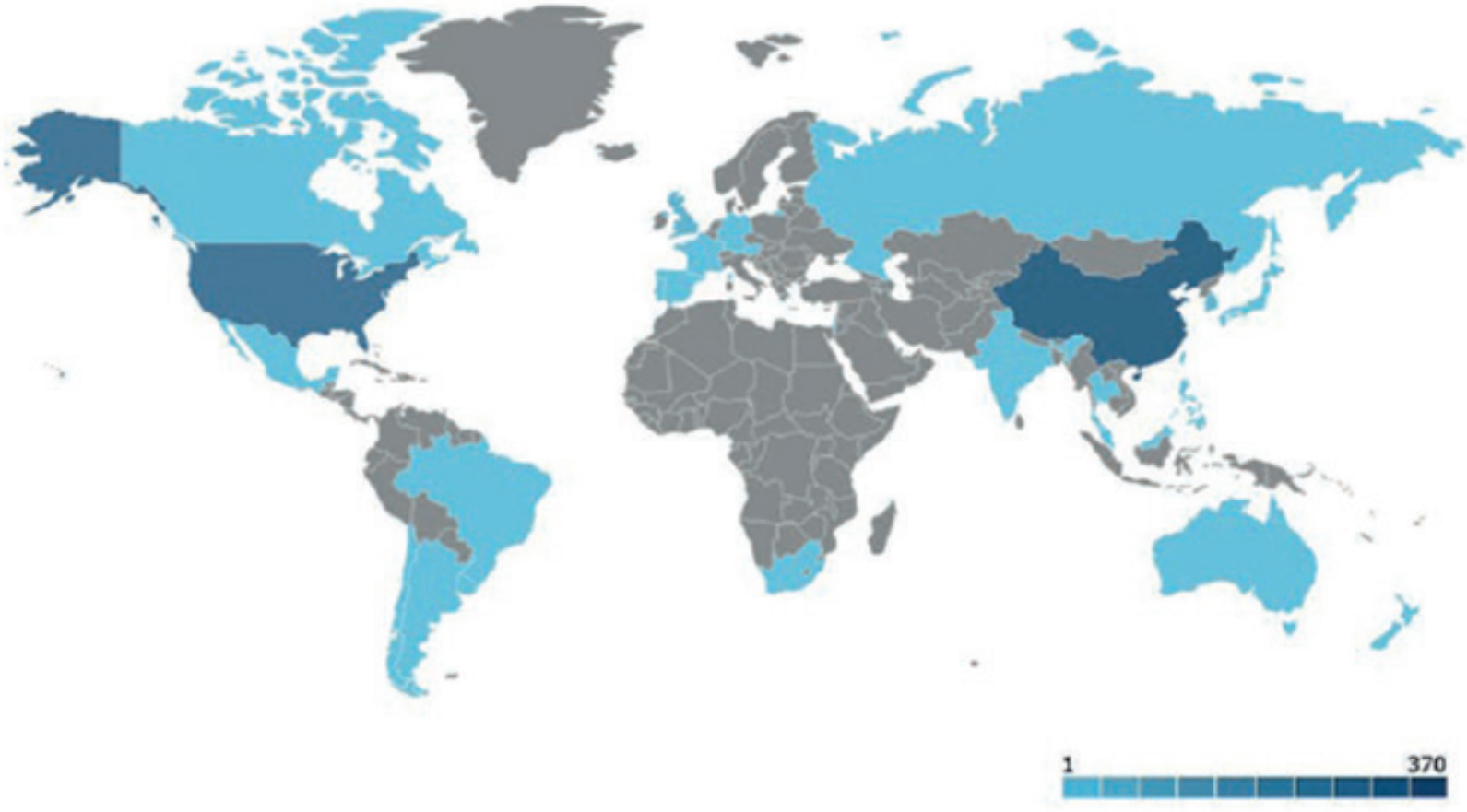
While the greatest density of patent filings has been in North America and China, applications are being filed across Europe, Asia, South America, and Australia.

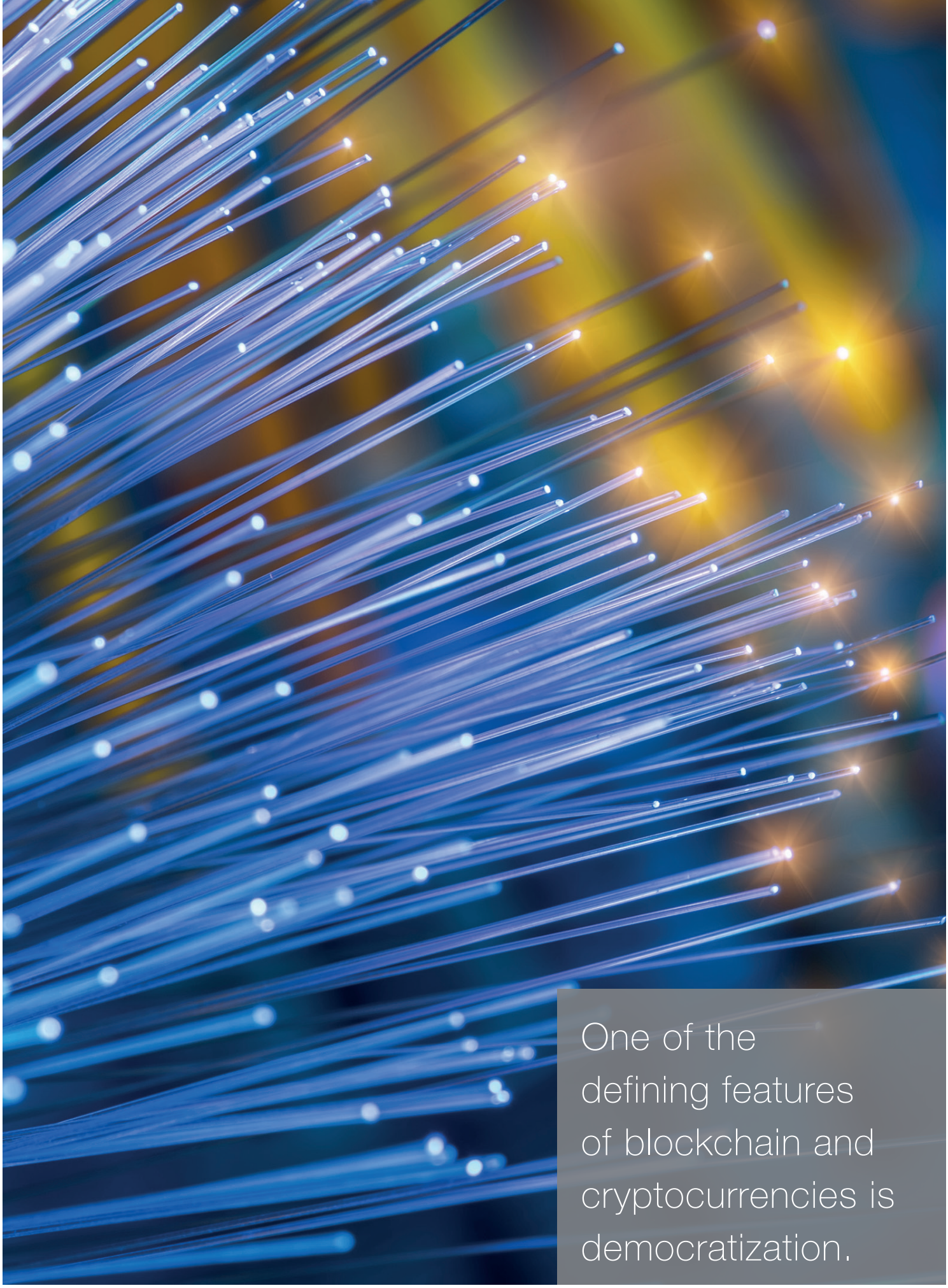
An international patent minefield is developing, and market participants with an international reach need to know their international exposure. And because of the international reach of most blockchain-rooted technologies, innovators should consider international protection for their inventions.



Empirical analysis of global published applications shows that the largest numbers of patent applications cluster around payment methods and systems using cryptocurrencies or the blockchain. 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 at the time of this writing, 400 patents (by family) directed to blockchain-related technologies have issued, another 2,205 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 to understand the risks presented by the IP of others in this emerging IP landscape.





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

Chapter 14 **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.

For example, ChangeTip, a former micropayment service, partnered with Direct Relief to enable donors to purchase $5 prenatal vitamin supplements for mothers in the developing world.[453] 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 DLT 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. [454]

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.[455] 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. Currently, the beta version of a platform called GiveTrackTM is live on the BitGive Foundation website.[456] 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.

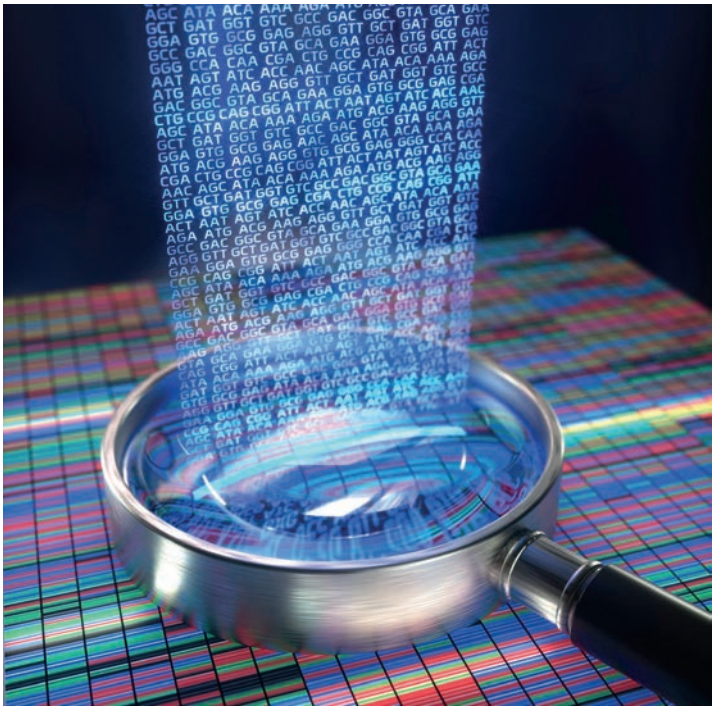
Access to financial services

Applications of the blockchain algorithm have much to offer the more than two 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 is said about the potential for Bitcoin to reduce fees for remittances,[457] 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.[458] For example, BitPesa focuses on converting bitcoins to Kenyan, Ugandan, or Tanzanian shillings or Nigerian naira and depositing that local currency to a mobile money number.[459] By relying on the preexisting mobile money wallet system in use by many Africans, 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 start-ups 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. [460] [461]

As with international aid, the blockchain algorithm has more to offer than simply reducing fees for money transfers. Coins.ph, one of the remittance start-ups in the Philippines highlighted above, has introduced a service called Teller.[462] Teller is like ridesharing for ATMs in that the Teller application connects customers to prescreened tellers who can take or distribute cash in exchange for bitcoins. Tellers and customers are held 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 algorithm, Teller can focus on the security and availability of only a single step of the process: the exchange of an electronic balance for cash. Using the blockchain algorithm, 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 algorithm opens up significant opportunities. For example, two projects started by an Afghan entrepreneur, Fereshteh Forough, use cryptocurrency[463] to pay Afghani women for work they complete as they learn skills for the digital economy. The Digital Citizens Fund[464] builds women-only computer centers to teach young women word processing, presentation, financial, and Internet-based tasks, while Code to Inspire 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. [466] With bitcoin, these young Afghani women can exercise a measure of control over their financial futures.

Blockchain-based services like WildSpark,[467] which compensates users for creating content, could further socioeconomic 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." [468]

The intersection of blockchain's potential impact and social investing is particularly evident in initial or independent coin offering.

Initial coin offerings

As we discussed in the chapter on application in capital markets, 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 preexisting cryptocurrencies like bitcoin. ICOs could have far-reaching implications for start-up ventures, nonprofits, and fundraising.

Various celebrities have publicized their support for ICOs.[469] Such high-profile activity raises a number of issues that would require

significant regulation from agencies such as the FTC and SEC.[470] 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.[471] In a November 2017 public statement, the SEC urged caution when considering investment in celebrity-backed ICOs. The SEC noted that celebrity endorsements may be unlawful if they lack certain disclosures and investment in such ICOs carry significant risk despite the celebrity's notoriety.[472]

Like equity crowdfunding – a disruption that eventually led to the passage of the JOBS Act[473] and other efforts to protect consumers engaging in social investment – ICOs have begun to garner attention from regulatory agencies such as the CFPB.

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.[474] With the increasing prevalence and popularity of ICOs,[475] 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.[476] Similarly, certain ICOs could eventually face actions from the FTC as they continue to be endorsed by social media influencers whose followers may seek them out as investment opportunities.[477] As such, the FTC may find it necessary to take action to prevent false advertising or other misleading behavior that could accompany some ICOs.4[78] The FTC emphasized the importance of this issue by holding a Decrypting Cryptocurrency Scams Workshop in June 2018.[479]

Blockchain, media, and advertising

Digital advertising ICOs[480] and initiatives such as Comcast's "Blockchain Insights Platform" seek to leverage blockchain technology to maximize ad targeting.[481] 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. [482]

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 Interactive Advertising Bureau released a whitepaper in February 2018 regarding how blockchain can revolutionize the digital advertising industry. [483] The concept proposed by the former ad network BitTeaser is an early example of what uses of this technology in the advertising sector may look like or what can be built upon. BitTeaser essentially set up an ad exchange where users could pay for ads and accept ad revenues in a variety of digital currencies, including bitcoin. [484]

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 radio-frequency identification (RFID) readers and tags.[485] 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 (for example, 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.[486] These technology-driven verification processes could encourage greater consumer confidence in purchases, while also reducing the risk of over-reliance on targeted advertising.

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 multitiered blockchains to keep transactions and messaging on the platform private.[487] 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.[488]

Improving governance and minimizing corruption

Blockchain may impact and modernize how information belonging to large groups of people or companies is stored and secured.[489] 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.[490] Countries such as Bermuda, Brazil, Georgia, Ghana, Honduras, India, Russia, and Rwanda have contemplated blockchain-based land registries.[491] In summer 2018, the Royal Gazette reported that Bermuda, in collaboration with the Bitfury Group, will add blockchain technology to its land registry system. [492]

Likewise, the U.S. title insurance industry could use blockchain to change how consumers buy and sell property. The Ethereum blockchain may be used 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. [493]

The state of Delaware launched the "Delaware Blockchain Initiative" in 2016 to explore ways to streamline corporate and governmental processes including incorporating blockchain technology in the handling of official documents, such as title documents and birth certificates. The state also passed amendments to its laws, such as allowing 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.[494] 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.[495]

Summary

The initial successes and challenges of using cryptocurrencies for social impact projects have inspired a new wave of innovation that is 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.

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 ten 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 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 PoW 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/cryptoasset

Tokens that are digital representations of value or utility within an ecosystem. Crypto 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 PoW 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 PoW.

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 PoW 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

The term “smart contract” can refer either to these coded instructions or to the natural language contracts, which rely on this underlying software for their execution. For clarity, the former can be referred to as “smart contract code” and the latter as a “smart legal contract.”

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.

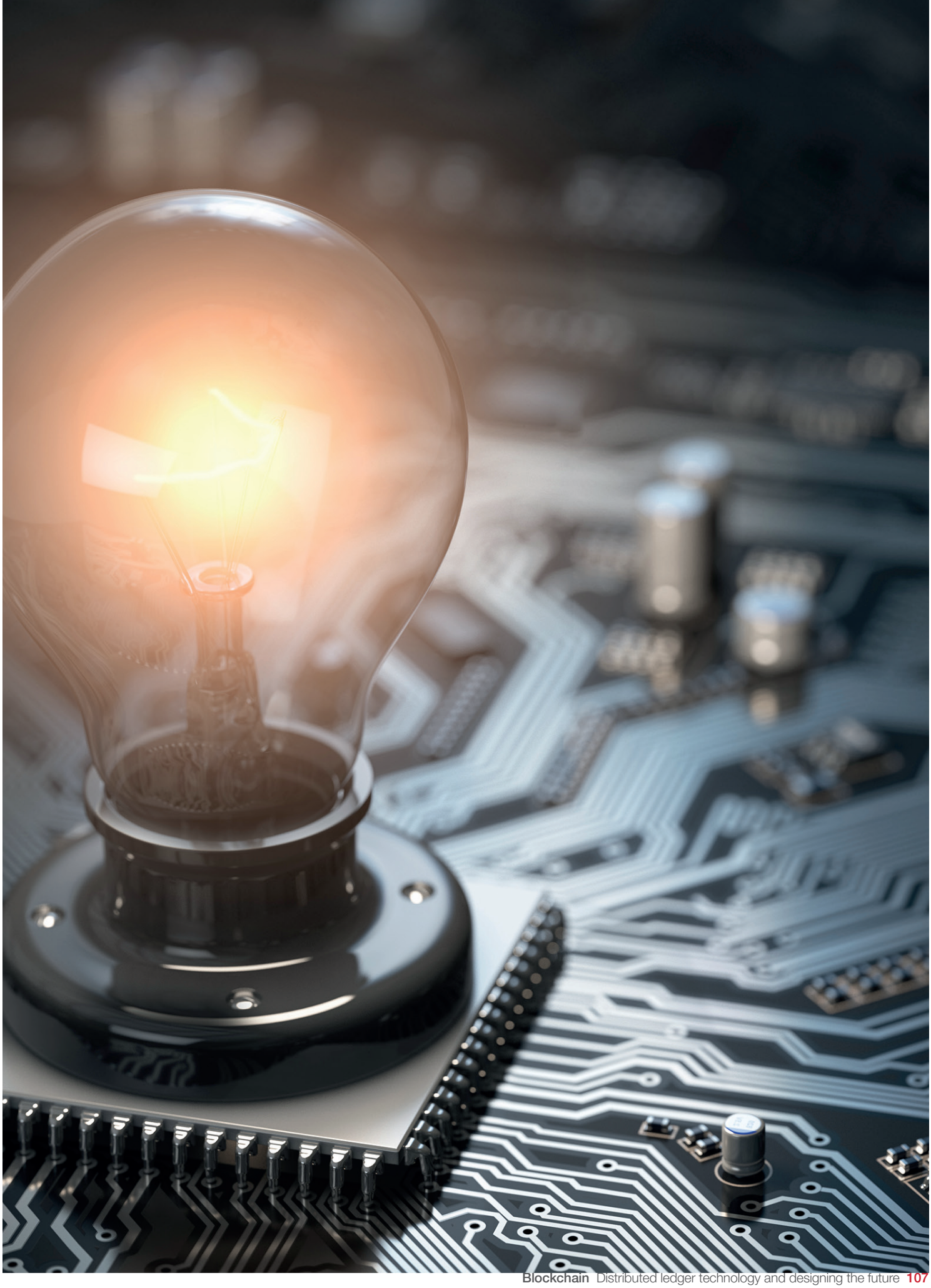
Virtual currency

Virtual currency is a legal or regulatory term of art. The European Fifth Money Laundering Directive define virtual currency as “digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and 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.”460

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.



Our team

FinTech Leadership

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

Global Corporate Group

Janet Bo Chun Cheung
Partner
Hong Kong
+1 212 549 0396
Janet.cheung@reedsmith.com

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

IP, Tech & Data

Gerard M. Donovan
Partner
Washington D.C.
+1 202 414 9224
gdonovan@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

Howard Womersley Smith
Partner
London
+44 (0)20 3116 3498
hwsmith@reedsmith.com

Xiaoyan Zhang
Counsel
San Francisco
+1 415 659 5957
xzhang@reedsmith.com

Jim Barbuto
Associate
New York
+1 212 549 4240
vbarbuto@reedsmith.com

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

Maria B. Earley
Partner
Washington, D.C.
+1 202 414 9302
mearley@reedsmith.com

C. Neil Gray
Partner
New York
+1 212 231 2652
cgray@reedsmith.com

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

Jeffrey D. Silberman
Counsel
New York
+1 212 549 4648
jsilberman@reedsmith.com

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

Jane Grinblat
Associate
Munich
+49 (0)89 20304 165
jgrinblat@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

Hagen Rooke
Counsel
Singapore
+65 6320 536
hrooke@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

Olga Newman
Associate
London
+44 (0)20 3116 3823
onewman@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 & Transportation

Richard M. Hakes
Partner
London
+44 (0)20 3116 2996
rhakes@reedsmith.com

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

Real Estate

James R. Eskilson
Partner
Century City
+1 310 734 5205
jeskilson@reedsmith.com

Endnotes

Chapter 1 – The mysterious origins of blockchain

1. http://fortune.com/2017/08/22/bitcoin-ethereum-blockchain-cryptocurrency/.

Chapter 2 – Blockchain 101

2. http://radar.oreilly.com/2015/01/understanding-the-blockchain.html.
3. https://bitcoin.org/bitcoin.pdf.
4. https://cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work.
5. 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.
6. "Bitcoin" with a capital B refers to the protocol or software, whereas "bitcoin" (lower case b) refers to the unit of currency.
7. "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.
8. https://www.cnbc.com/2017/05/26/cana-da-backs-off-blockchain-interbank-payment-system.html.
9. https://neo-ngd.github.io/reference/How-To-Become-NEO-Consensus-Node.html#governance-models.

Chapter 3 – Smart contracts

10. https://www.forbes.com/sites/bernardmarr/2018/02/02/blockchain-a-very-short-history-of-ethereum-everyone-should-read/#43381771e892.
11. https://thenextweb.com/hardfork/2018/11/14/record-art-sales-blockchain/.
12. Bryan Smith, "The Story of the DAO, and How it Shaped Ethereum," (May 23, 2018), Coin Insider, available at https://www.coininsider.com/what-happened-to-the-dao/.
13. https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf.
14. https://www.isda.org/2018/10/03/smart-derivatives-contracts-from-concept-to-construction/.
15. See figure 1 on page 3 of the ISDA smart derivatives contract white paper.
16. ISDA Common Domain Model Version 1.0 Design Definition Document (October 2017), https://www.isda.org/a/gVKDE/CDM-FINAL.pdf.
17. https://www.isda.org/a/MhgME/Legal-Guidelines-for-Smart-Derivatives-Contracts-Introduction.pdf.
18. https://www.isda.org/a/23iME/Legal-Guidelines-for-Smart-Derivatives-Contracts-ISDA-Master-Agreement.pdf.
19. https://www.cnbc.com/2016/04/19/barclays-used-blockchain-tech-to-trade-derivatives.html.
20. http://www.dtcc.com/news/2016/april/07/successful-blockchain-test-completed.
21. https://cftc.gov/About/Commissioners/JChristopherGiancarlo/index.htm.
22. https://cftc.gov/About/Commissioners/JChristopherGiancarlo/index.htm.
23. https://www.lawsociety.org.uk/news/stories/cryptoassets-dlt-and-smart-contracts-ukjt-consultation/.

Chapter 4 – Applications of DLT

24. https://www.coindesk.com/delaware-house-passes-historic-blockchain-regulation/
25. https://www.coindesk.com/arizona-smart-contract-clarity-winning-startups/
26. Tennessee: http://wapp.capitol.tn.gov/apps/Billinfo/default.aspx?BillNumber=SB1662&ga=110Wyoming: http://www.wyoleg.gov/2018/Introduced/HB0101.pdf
27. https://www.smh.com.au/business/markets/asx-delays-blockchain-transition-six-months-20180904-p501qq.html

Chapter 5 – U.S. regulatory landscape

28. 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.
29. Sydney Ember, "New York Proposes First State Regulations for Bitcoin," New York Times, DealBook (July 17, 2014), available at http://dealbook.nytimes.com/2014/07/17/lawsky-proposes-first-state-regulations-for-bitcoin/?_r=0.
30. 23 N.Y.C.R.R. Part 200 (Virtual Currencies), available at http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf (hereinafter, BitLicense).
31. Id.
32. See, for example, Daniel Roberts, "Bitcoin company ditches New York, blaming new regulations," Fortune (June 11, 2015), available at http://fortune.com/2015/06/11/bitcoin-shapeshift-newyork-bitlicense/.
33. BitLicense § 200.2(p).
34. Id. § 200.3(a).
35. Id. § 200.2(q).
36. Nermin Hajdarbegovic, "Lawsky: Bitcoin Developers and Miners Exempt from BitLicense," CoinDesk (October 15, 2014), available at http://www.coindesk.com/lawsky-bitcoin-developers-miners-exempt-bitlicense/.
37. Id.
38. BitLicense § 200.2(q).
39. Id. § 200.2(q)(1).
40. Id. §§ 200.3(a), 200.4, 200.5, 200.21.
41. Id. § 200.6.
42. Id.
43. Id. § 200.4(c).
44. Id. § 200.10.
45. Id. § 200.6.
46. Id. §§ 200.12(a), 200.15.
47. Id.
48. Id.
49. Id.
50. Id.
51. Id.
52. Id.
53. Id. § 200.8.
54. Id. § 200.9.
55. Id. § 200.12.
56. Id. § 200.19.
57. Id. § 200.20.
58. Id. § 200.18.
59. Id. § 200.19(g).
60. Id. § 200.16.
61. Id. § 200.17.
62. Id. § 200.13
63. Id. § 200.14.
64. A.B. 1326, Cal. Leg. 2015-2016 Reg. Sess. (Cal. 2015), available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1326.
65. Id.
66. Yessi Bello Perez, "California's Bitcoin Bill Shelved by State Senator," CoinDesk (September 16, 2015), available at http://www.coindesk.com/californias-bitcoin-bill-shelved-by-state-senator/; Brian Doherty, "California Bitcoin Regulatory Bill Pulled by its Sponsor," reason.com (August 22, 2016), available at http://reason.com/blog/2016/08/22/california-bitcoin-regulatory-bill-pulle.
67. Conn. Gen. Stat. § 36a-596(14).
68. Conn. Gen. Stat. §§ 36a-598(11); 600(c), (d), 602(a).
69. N.H. Rev. Stat. Ann. §§ 399-G:1(XVI)(b); 399-G:2.
70. N.H. Rev. Stat. Ann. §§ 399-G:1(VII), (XV).
71. New Hampshire House Bill 436 (2017), https://legiscan.com/NH/text/HB436/id/1456175.
72. Stan Higgins, "New Hampshire Governor Signs Bitcoin MSB Exemption Into Law," CoinDesk (June 7, 2017), available at http://www.coindesk.com/new-hampshire-governor-signs-bitcoin-msbexemption-law/.
73. N.C. Gen. Stat. § 53-208.42(20).
74. N.C. Gen. Stat. § 53-208.42(13)(b).
75. North Carolina Commissioner of Banks, Money Transmitter Frequently Asked Questions, available at http://www.nccob.gov/Public/financialinstitutions/mt/mtfaq.aspx (last visited April 20, 2017).
76. Pete Rizzo, "North Carolina Governor Signs Bitcoin Bill into Law," CoinDesk (July 6, 2016), available at http://www.coindesk.com/north-carolina-governor-signs-bitcoin-bill-law/.

77. Vic Lance, "Virtual Currency in Washington State: What Changes in July," CoinDesk (June 8, 2017), available at http://www.coindesk.com/virtual-currency-changes-washington-state-money-transmitter-law/.

78. Washington State Department of Financial Institutions, Bitcoin and Virtual Currency Regulation, http://www.dfi.wa.gov/bitcoin.

79. 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 (December 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 (November 30, 2016), available at https://www.idfpr. com/news/PDFs/DFPRRequestforCommentsDigitalCurrencyRegulatoryGuidance2016.pdf.

80. Illinois Department of Financial and Professional Regulation IDFPR: Request for Comment, Digital Currency Regulatory Guidance (November 30, 2016), available at https://www.idfpr. com/news/PDFs/IDFPRRequestforCommentsDigitalCurrencyRegulatoryGuidance2016.pdf.

81. Coinbase accounts – Hawaii (February 27, 2017), available at https://support.coinbase.com/customer/portal/articles/2754027.

82. Id.; Haw. Rev. Stat. § 489D-8.

83. N.C. Gen. Stat. § 53-208.42(17)(i).

84. Coinbase accounts – Hawaii (February 27, 2017), available at https://support.coinbase.com/customer/portal/articles/2754027.

85. Id.

86. State of Wisconsin Department of Financial Institutions, Sellers of Checks, https://www.wdfi.org/fi/lfs/soc/ (last accessed April 19, 2017).

87. Id.

88. 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.

89. Id.

90. "US State-level Digital Currency Law & Regulation," Merkle Tree, http://merkletree.io/blog/2015/07/us-state-level-digital-currency-law-regulation/.

91. Conference on State Bank Supervisors, State Regulatory Requirements for Virtual Currency Activities, CSBS Model Regulatory Framework (September 15, 2015), available at https://www.csbs.org/regulatory/ep/Documents/CSBS-Mod-el-Regulatory-Framework%28September%2015%202015%29.pdf.

92. Id.

93. "New State Blockchain Legislation," Reed Smith Client Alert (June 19, 2017), available at https://www.reedsmith.com/en/perspectives/2017/06/new-state-blockchain-legislation.

94. Id.

95. "Arizona's Blockchain Gun Tracking Bill is Close to Becoming Law," CoinDesk, April 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-gover-nor-enacts-law-including-blockchain-application.

96. S.B. 2601, 53d Leg., 2nd Reg Sess. (Ariz. 2018). See also "Arizona Law Would Define When ICOs Are Securities," CoinDesk, February 13, 2018, available at https://www.coindesk.com/arizona-law-define-icos-securities/.

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

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

99. "Illinois Partners with Evernym to Launch Birth Registration Pilot," The Illinois Blockchain Initiative (August 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 (August 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.
100. H.B. 0019, 64th Leg., 2018 Budget Sess. (Ariz. 2018).
101. H.B. 0070, 64th Leg., 2018 Budget Sess. (Ariz. 2018).
102. H.B. 0101, 64th Leg., 2018 Budget Sess. (Ariz. 2018).
103. S.F. 0111, 64th Leg., 2018 Budget Sess. (Ariz. 2018).
104. Colorado Department of Regulatory Agencies, Interim Guidance Cryptocurrency and the Money Transmitters Act (September 20, 2018), available at https://www.colorado.gov/pacific/dora/node/94326.
105. "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 (September 17, 2015), available at http://www.cftc.gov/PressRoom/PressReleases/pr7231-15 (hereinafter, Coinflip Settlement).
106. See generally Commodity Exchange Act, 49 Stat. 1491, 7 U.S.C. §§ 1, et seq.
107. 7 U.S.C. § 1a(9).
108. See, for example, U.S. Commodity Futures Trading Commission, Testimony of Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition & Forestry (December 10, 2014), available at http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6.
109. Coinflip Settlement.
110. LedgerX, LLC, Order of Registration (July 6, 2017), available at http://www.cftc.gov/PressRoom/PressReleases/pr758417; LedgerX, LLC Order of Registration (July 24, 2017), available at http://www.cftc.gov/idc/groups/public/@otherif/ documents/ifdocs/ledgerxdcoregorder72417.pdf.
111. http://www.cftc.gov/PressRoom/PressReleases/pr7654-17
112. http://www.cftc.gov/LabCFTC/index.htm 100 31C.F.R. § 1010.100(ff).
113. Colorado Department of Regulatory Agencies, Interim Guidance Cryptocurrency and the Money Transmitters Act (September 20, 2018), available at https://www.colorado.gov/pacific/dora/node/94326.
114. Id.
115. 31 C.F.R. § 1010.100(ff).
116. 31 C.F.R. § 1010.100(ff)(5)(i)(A) (emphasis added)
117. Letter from Drew Maloney, Assistant Sec'y of Legislative Affairs, Dep't of Treasury, to Ron Wyden, Senator, U.S. Senate (February 13, 2018).
118. 18 U.S.C. § 1960.
119. U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (March 18, 2013), available at https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.
120. Id.
121. U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Virtual Currency Mining Operations, FIN-2014-R001 (January 30, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R001.html.
122. U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (March 18, 2013), available at https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.
123. U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Virtual Currency Mining Operations, FIN-2014-R001 (January 30, 2014), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R001.html.
124. U.S. Department of the Treasury, FinCEN, Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity, FIN-2014-R002 (January 30, 2014), available at https://www.fincen.gov/news_room/ rp/rulings/html/FIN-2014-R002.html.
125. 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 (April 29, 2014), available at https://www.fincen.gov/news_ room/rp/rulings/html/FIN-2014-R007.html.

126. U.S. Department of the Treasury, FinCEN, Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform , FIN2014-R011 (October 27, 2014), available at https://www.fincen. gov/news_room/rp/rulings/html/FIN-2014-R011.html.

127. Id.

128. U.S. Department of the Treasury, FinCEN, Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, FIN2014-R012 (October 27, 2014), available at https://www.fincen. gov/news_room/rp/rulings/html/FIN-2014-R012.html.

129. 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 (August 14, 2015), available at https://www.fincen.gov/news_room/rp/rulings/html/FIN-2015-R001.html.

130. Letter from Drew Maloney, Assistant Sec'y of Legislative Affairs, Dep't of Treasury, to Ron Wyden, Senator, U.S. Senate (February 13, 2018). Proper citation should be "Maloney, supra note X, at X" in reference to the note above. However, the note number and page number are currently unknown because editing of the document is ongoing.

131. Id.

132. H.R. 6411, 115th Cong. (2018).

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

134. Id.

135. Id.

136. Id.

137. Id.

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

139. See, for example, Perianne Boring, "You Down with OCC? – Fin-Tech Firms See Promise in Special Bank Charter," Forbes (January 27, 2017), available at https://www.forbes.com/sites/perianne-boring/2017/01/27/you-down-with-occ-fintech-firms-see-promise-in-special-bank-charter/#78ad48db32e1.

140. 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 (January 17, 2017), available at http://www.dfs.ny.gov/about/occ_letter1-17-17.pdf.

141. 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. April 26, 2017), available at https://bankcsbs.files.wordpress.com/2017/04/csbs-occ-complaint-final.pdf.

142. 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.

143. "States Likely to Revive Challenge to OCC Fintech Charter," Bloomberg Law (August 1, 2018), available at https://www.bna.com/states-likely-revive-n73014481333/.

144. See, for example, Solis v. Latium Networks, Inc., No. 18-10255 (SDW) (SCM), 2018 WL 6445543 (D. N.J. Dec. 10, 2018); U.S. v. Zaslavskiy, No. 17-cr-00647-RJD, 2018 WL 4346339 (E.D.N.Y. September 11, 2018).

145. Letter from Jay Clayton to Representative Ted Budd, March 7, 2019, available at https://coincenter.org/files/2019-03/clayton-token-response.pdf.

146. Virtual Currencies: The Roles of the SEC and CFTC, Before the S. Comm. on Banking, Hous., Urban Affairs, 115th Cong. (2018) (statement of Jay Clayton, Chairman, U.S. SEC).

147. Id.

148. William Hinman, Dir., U.S. SEC, Remarks at Yahoo Finance All Markets Summit: Crypto (June 14, 2018), available at https://www.sec.gov/news/speech/speech-hinman-061418.

149. SEC, Public Statement on Framework for 'Investment Contract' Analysis of Digital Assets (April 3, 2019), available at https://www.sec.gov/news/public-statement/statement-framework-investment-contract-analysis-digital-assets.

150. Id.

151. SEC, Response of the Division of Corporation Finance Re: TurnKey Jet, Inc. (April 3, 2019), available at https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm.

152. Id.

153. Virtual Currencies: The Roles of the SEC and CFTC, Before the S. Comm. on Banking, Hous., Urban Affairs, 115th Cong. (2018) (statement of Jay Clayton, Chairman, U.S. SEC).

154. "SEC's Clayton: Use of a token can evolve toward or away from being a security," (April 12, 2018), available at https://coincenter.org/entry/sec-s-clayton-use-of-a-token-canevolve-toward-or-away-from-being-a-security.

155. Letter from Jay Clayton to Representative Ted Budd (March 7, 2019), available at https://coincenter.org/files/2019-03/clayton-token-response.pdf.

156. "Ethereum and Bitcoin Prices Jump After SEC Official Says Ether Is Not a Security," Fortune (June 14, 2018), available at http://fortune.com/2018/06/14/ethereum-price-sec-ruling-bitcoin-security/.

157. "SEC Chairman Jay Clayton Says Bitcoin Not a Security, Most ICOs Likely Are," Cointelegraph (June 6, 2018), available at https://cointelegraph.com/news/sec-chairman-jay-claytonsays-bitcoin-not-a-security-most-icos-likely-are.

158. "SEC Commissioner Cautions Against 'Blanket' ICO Classification", CoinDesk (May 9, 2018), available at https://www.coindesk.com/sec-commissioner-cautions-blanket-ico-classification/.

159. "SEC is cautiously open to initial coin offerings, commissioner says," CNBC (April 30, 2018), available at https://www.cnbc.com/2018/04/30/sec-is-cautious-but-open-to-crypto-fundraising-commissioner-says.html.

160. U.S. SEC, 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 (March 10, 2017), available at https://www.sec.gov/rules/sro/batsbzx/2017/34-80206.pdf.

161. Id. at 2.

162. Id.

163. Id.

164. Id. at 38.

165. U.S. SEC, 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 (March 28, 2017), available at https://www.sec.gov/rules/sro/ny-searca/2017/34-80319.pdf.

166. Arjun Kharpal, "Bitcoin marches towards all-time high as SEC gives potential second shot to Winklevoss ETF," CNBC (April 26, 2017), available at http://www.cnbc.com/2017/04/26/bitcoin-pricesec-winklevoss-etf-review.html.

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

168. https://www.sec.gov/rules/sro/nysearca/2017/34-82350.pdf

169. https://www.sec.gov/rules/sro/nysearca/2018/34-83904.pdf

170. https://www.sec.gov/rules/sro/cboebzx/2018/34-84231.pdf

171. SEC Release No. 81367 (August 9, 2017), available at https://www.sec.gov/litigation/suspensions/2017/34-81367.pdf.

172. SEC Release No. 81474 (August 23, 2017), available at https://www.sec.gov/litigation/suspensions/2017/34-81474.pdf.

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

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

175. "Regulators are Looking at Cryptocurrency," SEC Press Release: Statement by SEC Chairman Jay Clayton and CFTC Chairman J. Christopher Giancarlo (January 25, 2018).

176. https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.

177. "SEC subpoenas TechCrunch founder's cryptofund amid broader investigation into digital coins," CNBC (March 2, 2018), available at https://www.cnbc.com/2018/03/02/sec-subpoenas-techcrunch-founders-cryptofund-amid-broader-investigation-into-digital-coins.html.

178. See SEC v. Kik Interactive Inc., 1:19-cv-05244 (E.D.N.Y. June 4, 2019).

179. See SEC Release No. 2018-240 (October 18, 2018), available at https://www.sec.gov/news/press-release/2018-240.

180. SEC Release No. 2019-59 (April 24, 2019), available at https://www.sec.gov/news/press-release/2019-59.

181. Paragon Coin, Inc., Securities Act Release No. 10,574, Admin. Proc. File No. 3-18897 (November 16, 2018), available at https://www.sec.gov/litigation/admin/2018/33-10574.pdf.; CarrierEQ, Inc., Securities Act Release No. 10,575, Admin. Proc. File No. 3-18898 (November 16, 2018), https://www.sec.gov/litigation/admin/2018/33-10575.pdf.

182. Id.

183. SEC Release No 2019-15 (February 20, 2019), available at https://www.sec.gov/news/press-release/2019-15.

184. Pete Rizzo, "Blockstack Files With SEC to Raise $50 Million in Reg-A+ Crypto Token Sale," CoinDesk (April 11, 2019), available at https://www.coindesk.com/blockstack-to-raise-50-million-in-first-reg-a-crypto-token-sale.

185. 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 Internal Revenue Service (March 25, 2014), available at https://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance.

186. 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 (September 21, 2016), available at https://www.treasury.gov/tigta/auditreports/2016re-ports/201630083fr.pdf.

187. Kelly Phillips Erb, "IRS Wants Court Authority to Identify Bitcoin Users & Transactions at Coinbase," Forbes (November 21, 2016), available at https://www.forbes.com/sites/kellyphillip-serb/2016/11/21/irswants-court-authority-to-identify-bit-coin-users-transactionsat-coinbase/#2ac6c1055979.

188. 26 U.S.C. § 7609(f)(2).

189. Letter from Am. Inst. of CPAs to Internal Revenue Serv. (May 30, 2018), available at https://www.aicpa.org/content/dam/aicpa/advocacy/tax/downloadabledocuments/20180530-aicpa-comment-letter-on-notice-2014-21-virtual-currency.pdf.

190. Id.

191. FINRA, Distributed Ledger Technology: Implications of Blockchain for the Securities Industry (January 2017), available at http://www.finra.org/sites/default/files/FINRA_Block-chain_Report.pdf.

192. Fin. Indus. Regulatory Auth., FINRA Encourages Firms to Notify FINRA if They Engage in Activities Related to Digital Assets (2018), available at https://www.finra.org/sites/default/files/notice_doc_file_ref/Regulatory-Notice-18-20.pdf.

193. Id.

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

195. 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 (November 22, 2016).

196. CFPB Blog, BCFP Office of Innovation proposes "disclosure sandbox" for fintech companies to test new ways to inform consumers (September 13, 2018), available at https://www.consumerfinance.gov/about-us/blog/bcfp-office-innovation-proposes-disclosure-sandbox-fintech-companies-test-new-ways-inform-consumers/.

197. "BCFP Collaborates With Regulators Around The World To Create Global Financial Innovation Network," Press Release (August 7, 2018), available at https://www.consumerfinance.gov/about-us/newsroom/bcfp-collaborates-regulators-around-world-create-global-financial-innovation-network/.

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

199. 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), available at http://www.cftc.gov/Press-Room/PressReleases/pr7380-16.

200. 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.

201. CFTC v. McDonnell et al., Case No. 1:18-cv-00361 (E.D.N.Y. 2018)

202. "U.S. Judge Sides With CFTC on Virtual Currency Oversight," Reuters (September 26, 2018), available at https://www.reuters.com/article/us-usa-cftc-bitcoin/u-s-judge-sides-with-cftc-onvirtual-currency-oversight-idUSKCN1M62Z0.

203. 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), available at https://www.fincen.gov/news_room/nr/html/20150505.html.

204. https://www.fincen.gov/news/news-releases/fin-cen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware.

205. U.S. SEC, 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 (September 22, 2014), https://www.sec.gov/litigation/litreleases/2014/lr23090.htm.

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

207. U.S. SEC, "SEC Charges Bitcoin Entrepreneur With Offering Unregistered Securities," Press Release 2014-111 (June 3, 2014), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541972520.

208. U.S. SEC, Press Release 2015271, "SEC Charges Bitcoin Mining Companies" (December 1, 2015), https://www.sec.gov/news/pressrelease/2015-271. html.

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

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

211. United States v. Zaslavskiy, Case No. 17-CR-647 (EDNY 2018).

212. U.S. v. Zaslavskiy, No. 17-cr-00647-RJD, Sentencing Memorandum, ECF 50 (E.D.N.Y. May 15, 2019).

213. https://www.sec.gov/litigation/complaints/2017/comppr2017-comppr2017-219.pdf; https://www.sec.gov/litigation/admin/2017/33-10445.pdf.

214. https://www.sec.gov/news/press-release/2018-185.

215. U.S. SEC, "SEC Charges Digital Asset Hedge Fund Manager With Misrepresentations and Registration Failures," Release: 2018-186 (September 11, 2018), https://www.sec.gov/news/press-release/2018-186.

216. 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).

217. SEC v. Blockvest, LLC et al., 3:18-cv-02287-GPC-MSB, (S.D. Cal., October 3, 2018),

218. Id. at ECF 41 (November 27, 2018), https://www.fintechupdate.com/wp-content/uploads/sites/20/2018/12/SEC-v-Blockvest.pdf.

219. Id. at ECF 61 (February 14, 2019), https://www.fintechupdate.com/wp-content/uploads/sites/20/2019/03/SEC-v.-Blockvest-Order.pdf

220. Zachary Coburn, Exchange Act Release No. 84,553, Admin. Proc. File No. 3-18888 (November 8, 2018).

221. SEC v. Natural Diamond Investment Co., et al., 9:19-cv-80633-RLR -S.D. Fla. (May 19, 2019), available at http://www.sec.gov/litigation/complaints/2019/comp-pr2019-72.pdf.

222. SEC v. Kik Interactive Inc., 1:19-cv-05244 (E.D.N.Y. June 4, 2019), available at https://www.sec.gov/litigation/complaints/2019/comp-pr2019-87.pdf.

223. Fin. Indus. Regulatory Auth., FINRA Charges Broker with Fraud and Unlawful Distribution of Unregistered Cryptocurrency Securities (October 2, 2018, 8:30 PM), http://www.finra.org/newsroom/2018/finra-charges-broker-fraud-and-unlawful-distribution-unregistered-cryptocurrency.

224. Id.

225. Id.

226. Id.

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

228. "Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court," U.S. Attorney's Office for the Southern District of New York, Press Release (November 6, 2014), available at https://www.fbi. gov/newyork/press-releases/2014/operator-of-silk-road2.0-website-charged-in-manhattan-federal-court.

229. "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," U.S. Attorney's Office for the Southern District of New York, Press Release (January 20, 2015), available at http://www.justice.gov/usao-sdny/pr/bitcoin-exchanger-sentenced-manhattan-federal-court-four-years-prison-selling-nearly-1.

230. "FTC Shuts Down Promoters of Deceptive Cryptocurrency Schemes," FTC Press Release (March 16, 2018), available at https://www.ftc.gov/news-events/press-releases/2018/03/ftc-shuts-down-promoters-deceptive-cryptocurrency-schemes.

231. "North American Securities Administrators Association, State and Provincial Securities Regulators Conduct Coordinated International Crypto Crackdown," Press Release (May 21, 2018), available at http://www.nasaa.org/45121/state-and-provincial-securities-regulators-conduct-coordinated-international-crypto-crackdown-2/.

232. "Office of the Secretary of the Commonwealth of Massachusetts, Secretary Galvin Issues Orders in Connection with ICO Cryptocurrency Sweep," Press Release (March 27, 2018), available at https://www.sec.state.ma.us/sct/current/sctcryptocurrency/cryptocurrencyidx.htm.

233. "Texas State Securities Board, Emergency Order Entered Against Cryptocurrency Firm," Press Release (January 24, 2018), available at https://www.ssb.texas.gov/news-publications/emergency-order-entered-against-cryptocurrency-firm.

Chapter 6 – European financial regulatory landscape

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

235. Case C-264/14, Skatteverket v. David Hedqvist (October 22, 2015), available at http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d-2dc30dd8ccd881260ee4096a4a6a9b3d479002e. e34 KaxiLc3qMb40Rch0SaxuRbxn0?doclang=EN&tex- t=& pageIndex=0&part=1&mode=DOC&docid=170305&oc-c=first&dir=&cid=854516 (ECJ Ruling).

236. See infra, III.B.1

237. ECJ Ruling.

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

239. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD__web.pdf.

240. 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.

241. Id. at 5.

242. Id.

243. Id.

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

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

246. https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf

247. https://www.esma.europa.eu/press-news/esma-news/steven-maijoor-addresses-econ-committee-securitisation

248. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018X0601(02)&from=EN.

249. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf.

250. https://www.fca.org.uk/publication/consultation/cp19-03.pdf.

251. https://www.reedsmith.com/en/perspectives/2018/11/bit-by-bit-one-step-closer-to-regulation.

252. https://www.fca.org.uk/publication/policy/ps19-22.pdf.

253. https://www.fca.org.uk/publications/policy-statements/ps19-22-guidance-cryptoassets.

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

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

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

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

258. Central Bank of Iceland, "Significant risk attached to use of virtual currency" (March 19, 2014), available at http://www.cb.is/ publications-news-and-speeches/news-and-speeches/news/2014/03/19/Significant-risk-attached-to-use-of-virtu- al-currency/.

259. https://www.fca.org.uk/news/press-releases/financial-con-duct-authority-provides-update-regulatory-sandbox.

260. BaFin Leaflet, "Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer," (December 19, 2013), available at https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html.

261. "Initial Coin Offerings: Advisory letter on the classification of tokens as financial instruments", Ref. No. WA 11-QB 4100-2017/0010 available at https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl_hinweisschreiben_einordnung_ICOs_en.html.

262. Decision of the 4th Criminal Senate of the Higher Regional Court of Berlin (September 25, 2018) (Az: (4) 161 Ss28/18).

263. “Ent¬wurf ei¬nes Ge¬set¬zes zur Um¬set¬zung der Än-de¬rungs¬richt¬li¬nie zur Vier¬ten EU-Geld¬wä¬sche¬richt¬li¬nie (Richt¬li¬nie [EU] 2018/843)” (May 24, 2019), available at https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2019-05-24-Gesetz-4-EU-Geldwaescherichtlinie/0-Gesetz.html.

264. The Legislative Decree No. 90 (May 25, 2017).

265. FCA Press Release (November 14, 2017), available at https://www.fca.org.uk/news/news-stories/consumer-warning-about-risks-investing-cryptocurrency-cfds.

266. FCA Press Release (July 3, 2018), available https://www.fca.org.uk/news/press-releases/fca-reveals-fourth-round-successful-firms-its-regulatory-sandbox and https://www.fca.org.uk/publications/consultation-papers/global-financial-innovation-network.

267. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf.

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

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

Chapter 7 – Asian financial regulatory landscape

270. https://www.mas.gov.sg/schemes-and-initiatives/Project-Ubin.

271. https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220.

272. https://www.iras.gov.sg/irashome/uploadedFiles/IRASHome/GST/Draft%20e-Tax%20Guide%20_GST_Digital%20Payment%20Tokens.pdf.

273. https://www.dlapiper.com/en/japan/insights/publications/2017/12/japan-regulatory-update-on-virtual-currency-business/.

274. https://www.financemagnates.com/cryptocurrency/news/over-100-crypto-exchanges-seek-licenses-from-japans-fsa/.

275. https://www.reuters.com/article/us-japan-cryptocurrency-q-a/the-coincheck-hack-and-the-issue-with-crypto-assets-on-centralized-exchanges-idUSKBN1FI0K4.

276. https://www.fsa.go.jp/news/30/virtual_currency/20180810.html.

277. https://uk.reuters.com/article/us-japan-cryptocurrency/japan-grants-cryptocurrency-industry-self-regulatory-status-idUKKCN1MY10W.

278. https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201312300002&toolsflag=Y&dtable=News.

279. https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201401060003&toolsflag=Y&dtable=News.

280. https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380131.

281. https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201906270004&aplistdn=ou=news,ou= multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News.

282. https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=18PR126.

283. https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=18PR13.

284. https://www.sfc.hk/web/EN/news-and-announcements/policy-statements-and-announcements/reg-framework-virtual-asset-portfolios-managers-fund-distributors-trading-platform-operators.html.

285. http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c3762245/content.html.

286. http://www.miit.gov.cn/n1146290/n4388791/c5781140/content.html.

287. https://www.scmp.com/business/banking-finance/article/2129645/pboc-orders-banks-halt-banking-services-cryptocurrency.

288. https://www.businessinsider.com/china-eliminates-all-cryptocurrency-trading-2018-2.

289. http://www.chinadaily.com.cn/a/201801/05/WS5a4eb4cba31008cf16da527c.html.

290. https://www.bloomberg.com/news/articles/2019-04-09/china-plans-to-ban-cryptocurrency-mining-in-renewed-clampdown.

Chapter 8 – Rest of the world financial regulatory landscape

291. https://gulfnews.com/business/banking/uae-central-bank-clarifies-virtual-currency-ban-1.1971802#.

292. https://ripple.com/insights/ripple-and-saudi-arabian-monetary-authority-offer-pilot-program-for-saudi-banks/.

293. https://www.customs.gov.sa/en/node/1022.

294. https://www.bankingtech.com/2018/12/kuwait-plots-payment-system-and-digital-dinar/.

295. https://www.bloomberg.com/news/articles/2019-02-20/bahrain-offers-incubator-style-regulatory-program-for-crypto.

296. https://financialtribune.com/articles/economy-business-and-markets-world-economy/79459/iranian-banker-calls-for-cryptocurrency.

Chapter 9 – Insuring digital currency and digital currency business

297. In this chapter, references to "bitcoin" generally also refer to similar derivative cryptocurrencies.

298. SEC v. Shavers, No. 4:13CV416, 2013 WL 4028182, at *2 (E.D. Tex. August 6, 2013).

299. 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 (March 25, 2014), available at https://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance.

300. 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 (September 17, 2015), available at http://www.cftc.gov/PressRoom/PressReleases/pr7231-15 (hereinafter, Coinflip Settlement).

301. 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 (April 12, 2014), available at http://www.economist.com/news/finance-and-economics/21600736-chinese-regulators-make-life-hard-cryp-to-currencies-dream-dispelled.

302. See chapters 5 and 7 of this white paper, discussing security concerns particular to bitcoin; see also Lloyd's Bitcoin Report.

303. 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).

304. "Great American Insurance Group First to Offer Bitcoin Coverage to Commercial and Governmental Entities," Press Release (June 2, 2014), available at http://www.businesswire.com/news/home/20140602006331/en/Great-American-Insurance-Group-Offer-Bitcoin-Coverage.

305. Commercial Crime Policy form (ISO 2015), §D(1)(k).

306. "Include Virtual Currency as Money Endorsement," form CR 25 45 11 15 (ISO 2015).

307. Bitpay, Inc. v. Massachusetts Bay Ins. Co., No. 1:15-cv03238 (N.D. Ga.).

308. See, for example, 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. August 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); 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. August 1, 2017) (same).

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

310. https://www.bitgo.com/insurance. .

311. See supra note 8.

312. https://support.xapo.com/insurance.

Chapter 10 – Applications in capital markets

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

314. Edward Robinson and Matthew Leising, Blythe Masters Tells Banks the Blockchain Changes Everything, Bloomberg Business (August 31, 2015), http://www.bloomberg.com/ news/features/2015-09-01/blythe-masters-tells-banksthe-blockchain-changes-everything; Jemima Kelly, Nine of world's biggest banks join to form blockchain partnership, Reuters (September 15, 2015), http://www.reuters.com/ article/2015/09/15/us-banks-blockchain-idUSKCN0RF24M20150915#vbbT0RI-RCTT8TkRP.97.

315. Accenture, Blockchain in the Investment Bank (2015), available at https://www.accenture.com/t20150811T015521w /us-en/_acnmedia/Accenture/ Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_13/Accenture-Blockchain-Investment-Bank.pdf#zoom=50.

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

317. https://www.greenwich.com/greenwich-research/re-search-documents/greenwich-reports/2015/jul/is-digitalledger-tech-2015-gr.

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

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

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

321. Kristen Haunss, "LPC: Loan Market Pushes Forward to Cut Settlement Times," Reuters (May 12, 2016), available at http://www. reuters.com/article/us-loan-settlement-idUSKCN0Y323Yl.

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

323. Id.

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

325. http://www.dtcc.com/news/2016/april/07/successful-block-chain-test-completed.

326. http://www.coindesk.com/european-banks-select-ibm-block¬chain-small-business-platform/.

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

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

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

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

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

332. https://qz.com/1004892/the-bancor-ico-just-raised-153mil¬lion-on-ethereum-in-three-hours/.

333. https://www.forbes.com/sites/omribarzilay/2017/07/15/tezos232-million-ico-may-just-be-the-beginning/#13aa9c304c52.

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

335. https://www.coindesk.com/kik-ico-raises-98-million-butfalls¬short-of-target/.

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

337. "Considering an IPO? The costs of going and being public may surprise you," Strategy & Article (September 2012), available at https:// www.strategyand.pwc.com/media/file/Strategyand_ Consider-ing-an-IPO.pdf.

338. https://coinmarketcap.com/.

339. "Institutional Investors are Using Back Door for Crypto Purchases," Bloomberg Law (October 1, 2018), available at https://www.bloomberglaw.com/document/XC2BD-SHC000000?bwid=00000166-305e-dff1-a5ee-387e6e400000%26email=00000166-3011-d273-adfe-f777c8b-d0001%26emc=bslnw_hlt%3A1%26et=CURATED_HIGH-LIGHTS%26qid=5483987.

340. https://www.valuewalk.com/2017/08/cryptocurren-cy-hedge-funds-bitcoin-price/.

341. Id.

342. 15 U.S.C. §§ 77b(a)(1); 78d.

343. 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").

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

345. 15 U.S.C. §§ 77e(a); 77e(c).

346. 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).

347. Id. at 10.

348. William Hinman, Dir., U.S. SEC, Remarks at Yahoo Finance All Markets Summit: Crypto (June 14, 2018), available at https://www.sec.gov/news/speech/speech-hin-man-061418

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

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

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

352. https://www.coindesk.com/hong-kong-regulator-warns-ico-to-kens-may-securities/.

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

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

355. https://www.securities-administrators.ca/aboutcsa.as-px-?id=1555.

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

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

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

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

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

Chapter 11 – Blockchain innovation in energy, commodities, shipping, and trade finance

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

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

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

364. https://www.brooklyn.energy/.

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

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

367. https://www.economist.com/news/leaders/21717371-thatsno-reason-governments-stop-supporting-them-wind-andsolar-power-are-disrupting.

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

369. https://www.ofgem.gov.uk/publications-and-updates/switching-programme-and-retail-code-consolidation-proposed-changes-licences-and-industry-codes.

370. https://www.electron.org.uk/innovation-projects.

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

372. https://www.dropbox.com/sh/b7bkpkzx9p2d007/AAD4OBtQAI3pe322JPjlJa4za?dl=0&preview=LIOTAG_VOLTEX_WHITEPAPER_EN.pdf.

373. Id.

374. https://www.edie.net/news/8/Shell-invests-in-peer-to-peer-energy-trading-blockchain-platform/.

375. https://www.edie.net/news/8/London-startup-performs-UK-s-first-blockchain-energy-trade./

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

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

378. https://www.tiberiuscoin.com/.

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

380. https://enerchain.ponton.de/.

381. 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-thenext-market-for-blockchain.

382. https://www.engerati.com/smart-infrastructure/article/blockchain/scaling-blockchain-peer-peer-energy-trading.

383. http://www.mercuria.com/media-room/business-news/compelling-results-blockchain-oil-trade-test-ing-soci%C3%A9t%C3%A9-g%C3%A9n%C3%A9rale-and.

384. https://www.societegenerale.com/en/content/komgo-blockchain-platform-to-transform-commodities-trade-finance.

385. Finextra, “IBM, Natixis and Trafigura team on blockchain platform for oil trades,” (March 28, 2017), available at https://finextra.com/newsarticle/30350/ibm-natixis-and-trafigurateam-on-blockchain-platform-for-oil-trades.

386. https://www.societegenerale.com/en/content/komgo-blockchain-platform-to-transform-commodities-trade-finance.

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

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

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

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

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

392. "Could blockchain technology revolutionise shipping?" available at http://www.ship-technology.com/features/featurecould-blockchain-technology-revolutionise-shipping-5920391/.

393. Linex Systems, "HMM completes first blockchain pilot voyage" (September 7, 2017), available at https://ca.linexsystems.com/contents/transit/2048225065?user_ id =815745&log=6719bcf9c34cde1ac6b3 90b56d263d79&p=52918035&m=1&s=213975&org_id=390345.

394. http://fortune.com/2017/08/22/walmart-blockchain-ibmfood-nestle-unilever-tyson-dole./.

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

396. Richard Milne, "Moller-Maersk puts cost of cyber attack at up to $300m," Financial Times (August 16, 2017), available at https:// www.ft.com/content/a44ede7c-825f-11e7-a4ce15b2513cb3ff, and marinemec.com, "Blockchain would have prevented Maersk cyber attack," (June 30, 2017), available at http://www.marinemec.com/news/view,blockchain-would-have-prevented-maersk-cyber-attack_48287.htm.

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

398. Id.

399. "EY, Guardtime And Industry Participants Launch The World's First Marine Insurance Blockchain Platform" (September 8, 2017), available at: http://www. the-blockchain.com/2017/09/08/ey-guardtime-indus-try-participantslaunch-worlds-first-marine-insurance-blockchain-platform/.

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

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

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

403. Id. "There are so many rights, options and abilities in commercial 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."

404. "The blockchain revolution in trade finance," available at https://www.barclayscorporate.com/insight-and-research/trading-and-exporting/blockchain-revolution-in-trade-finance.html.

405. "Barclays and Wave complete world's first blockchain trade finance transaction," Financial Times (September 7, 2016), available at http://www.newsroom.barclays.com/r/3396/barclays_and_wave_complete_world_first_blockchain_trade#.

406. Phillip Silitschanu, "Streamlining Trade Finance With Blockchain Technology," available at https://www.americanexpress.com/ us/content/foreign-exchange/articles/blockchain-technology-to-streamline-trade-finance/.

407. "Rebooting a Digital Solution to Trade Finance" (October 21, 2018), available at https://www.bain.com/insights/rebooting-a-digital-solution-to-trade-finance/.

408. Sofia Lotto Persio, "Banks bring blockchain innovation to letters of credit" (August 10, 2016), available at https://www.gtreview.com/news/ asia/banks-blockchain-innovation-letters-of-credit/.

409. Sanne Wass, "50 banks and corporates complete Voltron

blockchain trial" (May 8, 2019) available at https://www.gtreview.com/news/fintech/50-banks-and-corporates-join-voltron-blockchain-trial/

410. Eleanor Wragg, "LC Lite launches blockchain platform to replace LCs" (February 7, 2019) available at https://www.gtreview.com/news/fintech/lc-lite-launches-blockchain-platform-to-replace-lcs/.

411. Sanne Wass, "Trade finance and the crowded blockchain ecosystem" (March 3, 2019) available at https://www.gtreview.com/magazine/volume-17-issue-2/trade-finance-crowded-blockchain-ecosystem/.

412. "14 banks using we.trade for global trade finance, breaking down trade barriers for business" (February 12, 2019), available at https://www.ibm.com/blogs/blockchain/2019/02/14-banks-and-400-companies-now-using-we-trade-for-global-trade-finance/.

413. "Rebooting a Digital Solution to Trade Finance" (October 21, 2018), available at https://www.bain.com/insights/rebooting-a-digital-solution-to-trade-finance/.

Chapter 12 – Privacy and re-identification on the blockchain

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

415. Id.

416. https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/.

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

418. https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/.

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

420. Id.

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

422. Ron Miller, "The promise of managing identity on the blockchain," TechCrunch (September 10, 2017), available at https://techcrunch.com/2017/09/10/the-promise-of-managing-identity-on-theblockchain/.

423. https://mashable.com/2015/01/28/redditor-muslim-cab-drivers/#:eyJzIjoidCIsImkiOiJfMnFtMDlwdGJ2ajZubWFjbiJ9.

424. Ahmend Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou (2015), Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts (College Park and Ithaca, NY: University of Maryland and Cornell University).

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

426. See https://www.getmonero.org/resources/moneropedia/stealthaddress.html.

427. https://www.coindesk.com/privacy-blockchain-headed/.

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

429. De-identification Standards, p. 6.

430. Id.

431. Id. at 17.

432. De-identification Standards, p. 17.

433. Id. at 17.

434. Id. at 22.

435. Id.

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

437. https://pokitdok.com/security/.

438. Ron Miller, "PokitDok teams with Intel on healthcare blockchain solution," TechCrunch (May 10, 2017), available at https://techcrunch.com/2017/05/10/pokitdok-teams-with-intel-on-healthcareblockchain-solution/.

439. Robert Hackett, "Why J.P. Morgan Chase Is Building a Blockchain on Ethereum," Fortune (October 4, 2016) available at http://fortune.com/2016/10/04/jp-morgan-chase-blockchain-ethereumquorum/.

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

441. Id.

442. Jeff John Roberts, "How Banks Will Stop Snoops From

Using the Blockchain to Front-Run Trades," Fortune (July 7, 2016), available at http://fortune.com/2016/07/07/blockchain-r3/.

443. See Cal. Civ. Code § 1798.105 (West) (Effective January 1, 2020).

Chapter 13 – Intellectual property

444. https://bitcoin.org/en/.

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

446. https://litecoin.org/.

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

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

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

450. Id.

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

452. © Questel Orbit 2017, reproduced with permission. Social impact, Responsibility and Media.

Chapter 14 – Social impact, responsibility, and media

453. Laura Shin, "ChangeTip And Direct Relief Launch Charitable Campaign Using Bitcoin," Forbes (August 19, 2015), available at http://www.forbes.com/sites/laurashin/2015/08/19/change-tipand-direct-relief-launch-charitable-campaign-using-bitcoin/.

454. Nikolai Kuznetsov, "How Emerging Markets And Blockchain Can Bring An End To Poverty," Forbes (July 24, 2017), available at https://www.forbes.com/sites/nikolaikuznetsov/2017/07/24/ howemerging-markets-and-blockchain-can-bring-an-endto-poverty/#464206d74a0c.

455. BitGive "About Us" (September 21, 2017) available at https://www.bitgivefoundation.org/about-us/.

456. https://www.givetrack.org/.

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

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

459. https://www.bitpesa.co/guide.

460. http://sendfriend.io/.

461. https://coins.ph/.

462. https://coins.ph/teller.

463. https://www.coindesk.com/afghanistan-ethereum-code-to-inspire-value./

464. http://www.digitalcitizenfund.org/.

465. http://codetoinspire.org/.

466. Carole Vaporean, "How learning to code can bring Afghan girls into the global tech marketplace," New York Times (September 7, 2015), available at http://nytlive.nytimes.com/womenintheworld/2015/09/07/ceos-afghan-citadel-teaches-women-in-afghanistan-how-to-code/.

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

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

469. https://bitcoinist.com/celebrity-endorsed-ico-projects-whereare-they-now/.

470. https://www.sec.gov/news/public-statement/statement-potentially-unlawful-promotion-icos.

471. https://www.ccn.com/boxing-legend-manny-pacquiao-latest-celebrity-to-turn-ico-promoter/.

472. SEC Public Statement, "SEC Statement Urging Caution Around Celebrity Backed ICOs," (November 1, 2017), available at https://www.sec.gov/news/public-statement/statement-potentially-unlawful-promotion-icos.

473. Michael del Castillo, "Who Needs VC? Ethereum and the JOBS Act Could Change Everything," CoinDesk (April 10, 2017), available at https://www.coindesk.com/jobs-act-ethereum-blockchain-capital/.

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

475. Michael del Castillo, "Who Needs VC? Ethereum and the JOBS Act Could Change Everything," CoinDesk (April 10, 2017), available at https://www.coindesk.com/jobs-act-ethereum-blockchain-capital/.

476. Joseph Young, "Crowdfunding vs. ICO: Experts Question Legitimacy and Guarantees of Initial Coin Offerings," The

Cointelegraph (October 20, 2016), available at https://cointelegraph.com/ news/crowdfunding-vs-ico-experts-question-legitimacy-and-guarantees-of-initial-coin-offerings.

477. Danny Bradbury, "Can the Blockchain Save Social Media Influencers?" Nasdaq (June 28, 2017), http://www.nasdaq.com/article/can-the-blockchain-save-social-media-influencerscm809474.

478. "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 Alert (March 15, 2017), available at https://www.reedsmith.com/en/perspectives/2017/03/federal-trade-commission-considers-the-implication.

479. https://www.ftc.gov/news-events/events-calendar/2018/06/decrypting-cryptocurrency-scams.

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

481. "Comcast's Advanced Advertising Group and Participants Announce Blockchain-based Technology Platform," Comcast (June 20, 2017), available at http://corporate.comcast.com/news-information/news-feed/comcasts-advanced-advertising-group-and-participants-announce-plans-for-blockchain-based-technology-platform-aimed-at-making-premiumvideo-advertising-more-efficient.

482. https://cointelegraph.com/news/blockchain-in-media-howblockchain-can-help-advertising.

483. https://www.iab.com/wp-content/uploads/2018/02/Blockchain_for_Video_Advertising_Publisher-Buyer_Use_Cases_2018-02.pdf.

484. https://adswikia.com/bitteaser-cpc/.

485. Rebecca Campbell, "Babyghost and VeChain: Fashion on the Blockchain," Bitcoin Magazine (October 18, 2016), https://bitcoinmagazine.com/articles/babyghost-and-vechain-fashionon-the-blockchain-1476807653/.

486. https://cointelegraph.com/news/de-beers-tracks-diamondswith-blockchain-for-the-first-time.

487. Steve Olenski, "Will Blockchain Reinvent Social Media?" Forbes (August 9, 2017), available at https://www.forbes.com/sites/steveolenski/2017/08/09/will-blockchain-reinvent-social-media/#5b562b383ec1.

488. Id.

489. Jon Berkeley, "The Trust Machine," The Economist (October 31, 2015), available at http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine.

490. https://www.nytimes.com/2018/06/27/business/dealbook/governments-blockchains-services.html.

491. http://www.govtech.com/computing/Blockchain-Based-Property-Registries-May-Help-Lift-Poor-People-Out-of-Poverty.html.

492. http://www.royalgazette.com/business/article/20180628/bermudas-land-registry-to-go-on-blockchain.

493. Jen Wieczner, "Why Ethereum is Much More Valuable Than Bitcoin: SoFi CEO," Fortune (July 19, 2017), available at http://fortune.com/2017/07/19/bitcoin-ethereum-blockchain-sofi/.

494. https://strategiccoin.com/blockchain-for-loyalty-programs/.

495. Shareen Pathak, "How blockchain might be useful in marketing and advertising," Digiday (December 15, 2016), available at https://digiday.com/marketing/blockchain-tech-might-useful-marketing/.

Phone: +44 (0)20 3116 3000
Fax: +44 (0)20 3116 3999
DX 1066 City/DX18 London

ABU DHABI
ATHENS
AUSTIN
BEIJING
CENTURY CITY
CHICAGO
DALLAS
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