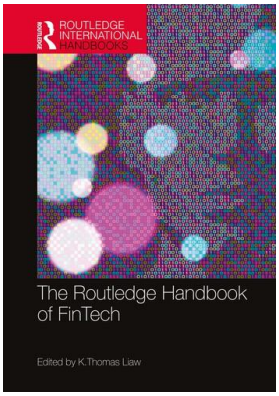

The Routledge Handbook of FinTech

K. Thomas

Distributed ledger technologies and blockchain for FinTech

Publication details
https://test.routledgehandbooks.com/doi/10.4324/9780429292903-8
Raghava Rao Mukkamala, Ravi Vatrapu
Published online on: 15 Jun 2021

6

DISTRIBUTED LEDGER TECHNOLOGIES AND BLOCKCHAIN FOR FINTECH

Principles and applications

Raghava Rao Mukkamala and Ravi Vatrapu

1 Introduction

Historically, technology advancements and financial innovations have been interlinked. In the recent past, technological innovations have played a crucial role in financial innovations that led to not only new forms of products and services but also disruption and disintermediation in the wider financial sector. One of the enduring impacts of the global Financial Crisis (GFC) has been the trust deficit between consumers and companies in the financial sector in general and the banking sector in particular. This erosion of institutional trust extended from the established players such as retail and investment banks to other centralized organizations such as central banks. One consequence of this has been the proliferation of FinTech entities that offer decentralized trust mechanisms and alternatives to fiat currencies. Due to their unique technological features such as the lack of centralized control and high level of anonymity, distributed ledger technologies (DLT) underpin much of the FinTech innovation and entrepreneurship and empower the evolution of decentralized applications in multiple domains such as finance, health care, supply chains etc. In this chapter, we present the underlying technical principles of DLT and blockchain technology and outline their practical applications to FinTech.

According to a World Bank report (Natarajan et al., 2019), with the rapid development and spread of new technological advancements, the finance sector is undergoing a significant transformation to embrace these innovations for the betterment of existing and innovation of new financial products and services. Blockchain technology came into the limelight when Bitcoin, a decentralized digital cash system was introduced as a peer- to-peer cryptocurrency in 2009 (Nakamoto, 2008) and as of 2020, Bitcoin is the largest cryptocurrency with a market capitalization of approximately more than 100 billion USD.[1] Moreover, an important feature of Bitcoin is maintainability of its currency value without any central authority or governmental administration but purely based on the transactions that are stored in the public distributed ledger (datastore) using blockchain technology. When Bitcoin was making its initial buzz, many institutions and people thought that it would not make any significant impact on the global economy; this was supported by several reports (European Central Bank, 2012; European Central Bank, 2015). However, such a view has changed drastically

in the last few years, especially with regards to cryptocurrencies; many financial institutions like banks started to explore and test the technologies behind blockchain and DLTs. Apart from Bitcoin, several hundred more cryptocurrencies were introduced, with a market cap of more than a couple of hundred billion dollars.[2] However the interest shown towards DLT and blockchain technologies is not only limited to the domain of finance; it has also garnered attention from many sectors like power generation, health, education, government, supply chain and logistics, transportation and others. The new technology has also inspired many people and organizations, resulting in fortunes for some entities and people and bankruptcy for others, for example cryptocurrency exchanges (Szostek, 2019).

Due to their innovative and disruptive nature, blockchain technologies have captured the attention of many governmental organizations, the academic community, enterprises and financial institutions. For example, the European Union has taken several initiatives to promote and harness the innovative technology. One such is the EU Blockchain Observatory & Forum,[3] started in 2018 by the European Union to promote collaboration between various initiatives on blockchain technologies among the member countries and also to highlight the important progress made in these technologies and at the same time promote education and awareness among the population and organizations. At the same time, since the cryptocurrencies provide high-level anonymity for their users, they became go-to currencies for illicit activities such as money laundering and cybercriminal activities (Sun Yin et al., 2019). Therefore, there is a strong desire on the part of regulatory authorities to initiate more regulatory guidance concerning DLTs and blockchain-based applications.

To understand the kind of impact DLT and blockchain technologies can have on FinTech, it is important to understand the technological foundations of the DLTs and blockchain, and the main principles and applications behind these technologies. It is also necessary to understand the current legal and regulatory initiatives concerning DLT and blockchain to foresee what kind of impact those will bring into the FinTech domain in terms of legal regulatory frameworks. Therefore, in this chapter we focus on the principles and the concepts behind DLT and blockchain in sec. 2. In the next section (sec. 3) various FinTech applications and their suitability concerning blockchain will be discussed. Then we turn our focus on legal and regulatory aspects of DLT and blockchain technologies in sec. 4. Final we conclude in sec. 5 with few comments about the market adoption of these technologies in FinTech.

2 Principles behind distributed ledger technologies and blockchain

The disruptive and innovative nature of blockchain technology resulted in the evolution of many decentralized applications such as cryptocurrencies and smart contracts. Bitcoin, a decentralized cryptocurrency based on blockchain technology was introduced in 2009 (Nakamoto, 2008) and in 2020 Bitcoin is the largest cryptocurrency with a market capitalization of approximately more than 200 billion USD.[4] Even though bitcoin is considered an innovative and disruptive technology, its underlying technical foundations and those of other cryptocurrencies actually originated back in the 1980–1990s (Narayanan and Clark, 2017b). The following is a brief description of various concepts and underlying technical components of DLT and blockchain technologies.

2.1 DLT and blockchain

According to Rauchs et al. (2018, p. 15), "Distributed ledger technology (DLT) has established itself as an umbrella term to designate multi-party systems that operate in an

environment with no central operator or authority, despite parties who may be unreliable or malicious ('adversarial environment')". The notion of DLT systems evolved in the 1980s in distributed computing and in that context a DLT system can be considered as a distributed datastore using state machine replication, where multiple parties operate in a decentralized environment without any central authority, communicate the atomic and incremental changes to the global state. Blockchain is a subset of DLT technologies. Even though the notion of blockchain evolved around the 1990s, it only became popular after 2009 when bitcoin cryptocurrency (Nakamoto, 2008) was introduced. Blockchain is the decentralized distributed data structure that is combined with guarantees against the tamper-resistance of transactions/records using cryptographic methods. By using the time-stamping of its transactions and messages, blockchain provides universally verifiable proofs for the existence or absence of a transaction in the distributed database, and the underlying cryptographic primitives, using hash functions and digital signatures, provide a guarantee that these proofs are computationally secure and verifiable at any point in time. Blockchain is decentralized, jointly maintained by a plurality of independent parties/nodes, and achieves consistency of transactions among distributed nodes by using distributed consensus protocols (such as Byzantine fault tolerance algorithm (Lamport et al., 1982)) without the need of having a central authority. In this chapter, we confine our discussion mostly to blockchain applications which will have practical relevance to FinTech rather than focusing DLTs which are mostly confined to the distributed computing domain.

2.2 Distributed ledger

The central idea of blockchain and DLT is the distributed and decentralized ledger maintained by several participating entities. The main difference between a centralized and decentralized ledger is the way it is maintained and how consensus is achieved. In the case of a centralized ledger, since it is maintained by a trusted central authority (such as a bank or a financial institution) there is no need for consensus. However, a distributed ledger is a global data structure that is collectively maintained by the participants who may not trust each other in decentralized environments on the Internet. Therefore, distributed ledgers need certain characteristics to maintain the integrity and consistency of the ledger. First of all, the ledger must be *immutable* in the sense that it only allows for new data to be appended, i.e. it neither allows deletion nor modifications to the ledger. Secondly, it should be possible to compute a succinct cryptographic digest to the state of the ledger for verification purposes, so that rather than storing the entire state of the ledger, the digest can be used to verify the state of the ledger, for example, to make sure that the ledger has not been tampered with. Built on the concept of peer-to-peer networks and distributed storage (Xu, 1999), distributed ledgers can be considered as a distributed data store with state machine replication using a peer-to-peer protocol, where transactions are atomic changes to the data store which are grouped into blocks (Mamoshina et al., 2018).

2.3 Hash functions

Hashing is known as a one-way function used to ensure the integrity of data. A hash function is an input independent average linear time algorithm that takes a set of variables or data and transforms it into a fixed size hash digest (Carter and Wegman, 1979). A successful hash function has the following characteristics. It is *deterministic* – the same input always creates the same output, *efficient* – output is computed in a timely manner, *distributed* – evenly spread

across the output range, meaning that similar data should not correlate to similar hashes, *preimage-resistant* – it will be impossible to find the input document x, based on the hash value ($h(x)$) and nearly *collision resistant* – no two different inputs x and y create the same hash $h(x) = h(y) \Longrightarrow x \equiv y$. Furthermore, hash functions are used for organizing and linking data together in blockchains. Today's cryptographic hash functions are built on certain standards, a particularly popular one is SHA-2 (Penard and van Werkhoven, 2008), a version of it (SHA-256) being used in the bitcoin blockchain. SHA-2 was developed partly by the United States National Security Agency (NSA) and it builds on two concepts: Merkle-Damg°ard construction (Merkle, 1989; Damg°ard, 1989) and Davies-Meyer compression (Simmons, 1994). Other common cryptographic standards include SHA-3 (Dworkin, 2015), Blake, and MD5. Another key concept of hash functions in the blockchain is that of organizing and linking data together. This is done through the hashing of various elements in the block header containing a hash of the previous block, Merkle root of transactions, time, and nonce. The concept of the Merkle Tree (Merkle, 1980) is that each transaction is hashed, then the resulting hash of each transaction is hashed to build a tree structure until the top node known as the Merkle root is obtained. This type of organizing of data allows secure and efficient verification of contents of a block and summarizes all the transactions in a block (Antonopoulos, 2014).

2.4 Digital signatures

One of the main goals of blockchain technology is to be able to verify the authenticity and non-repudiation of data/transactions. The digital signature is a cryptographic scheme that guarantees two properties: *authenticity*, that the data/message created or owned by the known sender and the *non-repudiation* property guarantees that the data is not altered, using a pair of keys with an asymmetric cryptographic algorithm like Rivest–Shamir–Adleman or RSA algorithm (Rivest et al., 1978). In the asymmetric cryptographic algorithm, two corresponding keys (e.g. public and private) will be generated and the data encrypted with one key can only be decrypted with the other corresponding key. Participants in the blockchain network use a public/private key pair, where the public key is used as an address to digital assets (such as coins in cryptocurrency) and the private key is used to claim the ownership over these digital assets (e.g. to spend coins in cryptocurrencies). Over the years, more secure versions of digital signatures have been developed. For instance, bitcoin uses the Elliptic Curve Digital Signature Algorithm (ECDSA) for key generation (Johnson et al., 2001).

2.5 Digital timestamping

The concept behind the distributed ledger data structure is adopted from digital timestamping and was proposed by Haber and Stornetta (1990) and Bayer et al. (1993) in the 1990s to address the challenges of a digital notary service that provides proof to establish that the documents were signed at a certain point in time and no later than that (Narayanan and Clark, 2017b). In the proposal made by Haber and Stornetta (1990), the documents were created and broadcasted continuously and the creator of a new document would sign the document digitally, attach the timestamp and then link the newly created document with the previously broadcasted document. Since the previous broadcasted document had been created and signed by someone else, this created long-chain documents authored by many participants

in a collaborative manner. The link between the documents is created using hashing rather than digital signatures, as the hash values of the document are quick and efficient to compute. Moreover, it was also proposed that documents created around the same time can be grouped into some kind of block structure so that these documents will have the same timestamp. The documents inside a block are linked by a binary tree of hash pointers known as a Merkle Tree (Merkle, 1980), which is an efficient data structure for the storage of hash values of documents (Narayanan and Clark, 2017b).

2.6 Fault tolerance

The requirements of a distributed ledger are much more stringent when compared to a centralized ledger due to the absence of a central authority. The distributed ledger has to deal with issues such as that participating nodes in the network may fail, or be malicious; it also needs to account for latency in the network and, therefore, achieving consensus in distributed ledgers is more challenging. There is a significant amount of research in fault-tolerant distributed computing (Lamport et al., 1982; Lamport, 2019; Lamport et al., 2001; Castro et al., 1999) where the problem of achieving state replication across different distributed nodes is explored. Several fault tolerance protocols like Paxos (Lamport et al., 2001), Practical Byzantine Fault Tolerance (PBFT) (Castro et al., 1999) and other protocols have contributed to some of the main ideas behind the fault-tolerance mechanisms blockchain and DLTs.

2.7 Consensus protocols

In order to avoid having a central authority for enabling trust in the system, there needs to be some mechanism that establishes trust between the involved parties, which is achievable by distributed consensus of those parties. In a blockchain, trust is ensured through a distributed consensus protocol. Although the protocol can vary slightly from system to system, the idea of achieving trust with the consensus of those parties involved remains the same. The two most widespread concepts in the distributed consensus protocol are proof-of-work and proof-of-stake.

Proof-of-work (PoW) refers to the idea that a service requester is required to solve a cryptographic puzzle (*computational work*) to participate in a network and it was initially proposed in hashcash (Back, 2002) as a countermeasure for denial of service attack using CPU (Central Processing Unit) cost-functions. In blockchain and especially in bitcoin (Nakamoto, 2008), it is used as a verification technique for finding the appropriate header for new blocks of data and to append them to the chain of blocks. To add a block, a node has to solve a cost-function (find the right *nonce*), that results in a pre-defined hash format with certain restrictions. At the same time, blocks can only be added to the longest chain (with the most proof-of-work invested), to avoid 'dishonest' attempts at altering the ledger. The concept of using a cost-function as a proof-of-work was first proposed by Adam Back in 2002.

Proof-of-stake (PoS) is another method for verifying and adding blocks to the blockchain, where the node that creates the next block is chosen (Wang et al., 2019). Therefore, a node adds and verifies blocks according to how much stake they have in the system. Thereby, ownership will lead to actors behaving honestly, because they would lose their stake if they behaved dishonestly. There are a few other consensus protocols such as proof of burn, proof of luck, elapsed-time and ownership; for more details about these consensuses, protocols can be found in (Wang et al., 2019).

2.8 Smart contracts

Using blockchain as a tamper-proof ledger would record the transfer and prove ownership of assets beyond any doubt. This enables smart contracts, an idea that was conceptualized already 20 years ago (Szabo, 1997) in the creation of computer programs that can securely enforce previously closed contracts in a decentralized manner. The idea of smart contracts is to take contractual clauses, translate them into code, thereby making them self-enforceable. Hence, intermediaries who are responsible for enforcing the contract are not needed, but instead, a trusted computer program is relied upon. Complex contractual and payment agreements can be included in standardized contracts and then be monitored and executed at low transactional costs, as they are managed digitally and immutably (Swan, 2015). Smart contracts will become powerful when combined with cryptocurrency platforms as they can be executed to handle money such as transferring money from one account to other (Narayanan and Clark, 2017b).

2.9 Public verses permissioned

One of the major design choices in blockchain and DLT is whether the network runs in a permission-less mode or a permissioned mode. Public blockchain and DLT like bitcoin and Ethereum are permissionless in the sense that anybody can join the network and perform transactions without any prior approval. Alternatively, in the permissioned blockchains, like Ripple, Corda, Hyperledger, an entity, a consortium or a central administrator controls access to the participants and assigns privileges to various participants based on the role they play in the blockchain ecosystem. One of the best advantages of permissioned blockchains is that, since all the participants are prescreened/known ahead/trusted, there is no need to adopt very expensive and computing-intensive consensus mechanisms like proof-of-work; on the contrary, a very simple mechanism can be adopted to achieve consensus among the participants. The orchestration of all the above-described technologies lead to the following characteristics (Faber et al., 2019) in blockchain as shown in Table 6.1.

3 Applications of DLT in FinTech

In this section, we focus our discussion on various applications in the FinTech domain where blockchain technology can make a significant impact in the coming years.

3.1 Cryptocurrencies

There were several attempts since the 1990s to create a decentralized digital currency which would be resistant to censorship, and able to protect itself against outside attacks. Some of

Table 6.1 Characteristics of the blockchain

Immutability	Data written to database cannot be changed or deleted without consensus leading to data integrity
Decentralization	No single point of failure/control achieved by decentralized architecture and a distributed database
Transparency	All data sent through the blockchain is visible to all network participants
Pseudonymity	The identity of data senders and receivers is unknown
Chronology	Every transaction is time-stamped and can be traced back

the notable attempts are the payment solutions such as b-money,[5] Hashcash (Narayanan and Clark, 2017a), and Bitgold,[6]. However, these attempts ended in failure, even though they came a bit closer to the main motivation. On Halloween in 2008, the Cypherpunk member (or group of members) under the pseudonym of Satoshi Nakamoto released a *whitepaper* on bitcoin (Nakamoto, 2008); this was essentially a detailed document outlining the technical and logical workings of blockchain. One of the members of Cypherpunk, Hal Finney, started engaging in conversation with Satoshi, and in 2009 received the first prototype from him (Chohan, 2017). After running the software, Hal Finney mined the first bitcoins and performed the first peer-to-peer blockchain transactions. Although conceived in the perfect storm after the 2008 financial crisis, and promising liberation from banking, bitcoin's first real use case was its manifestation as a black-market payment, secretive and essentially cost free – a reputation that it still carries to this day.

As of 2020, the total market cap of cryptocurrencies is $335 billion,[7] out of which the top 20 of the 2,500 live coins make up 90% of the value. It was not until 2014 when the banking world caught onto the underlying technology, that 'blockchain' as a term was even propagated. For the last few years, a unanimous belief in blockchain dealing with universal issues like corruption, inefficiency, and malfeasance has grown. The concept of blockchain has since merged with other areas of cryptography, peer-to-peer networking and economics, to form variants of the system more applicable to the financial sector (Treleaven et al., 2017). Obstacles to faster adoption remain within the areas of cyber risks, transaction delays due to scalability problems and high volatility, however, work is being done in solving these issues.

3.1.1 Cyber risk

The nature of blockchain-based technologies is that they are hard to tamper with. Since the data is linked using hash pointers any modifications to data in a blockchain can be easily identified. However, hashing and the storage of private-keys can be a weak point. Massachusetts Institute of Technology's Digital Currency Initiative (DCI) found that the IOTA project, whereby payments across interconnected devices happen through their cryptocurrency, was using an in-house created hash function Curl-P-27 that had some security lapses (Heilman et al., 2019), including that its function lacked a so-called seed-generator to help users generate keys for their wallets. Publishing of the cryptoanalysis of Curl-P-27 and other attacks on IOTA cryptocurrency (Heilman et al., 2019) have caused user losses amounting to 4 million USD worth of IOTA cryptocurrency. The DCI has pointed out that such architectural issues can be avoided by using well-established and scrutinized open-source functions available, and disadvise creating proprietary software which is not studied well enough or verified by cryptoanalysis. Crypto-dedicated security audits – such as SmartDec,[8] OpenZeppelin,[9] and Chainsecurity[10] are also being used more readily.

3.1.2 Transaction delays and scalability

The issue of scalability of cryptocurrencies comes from its consensus mechanisms. Since the cryptocurrencies operate in a decentralized fashion, they use a consensus mechanism to achieve an agreement between nodes. Bitcoin's proof-of-work can only process seven transactions per second, and Native Ethereum can process four transactions per second (Dalvit, 2020). However, new proof algorithms and techniques such as Zero-Knowledge Proofs (Goldwasser et al., 1989) and ZK-STARKS (Ben-Sasson et al., 2019) are being developed which allow for faster transaction times through better consensus. StarkWare,[11] a team made

up of developers from various groups such as ConsensSys, Coinbase, Intel Capital and researchers have developed a payment system on Ethereum called Stark allowing for 9,000 trades and 18,000 payments per second.

3.1.3 Volatility

Volatility in cryptocurrencies is one of the biggest issues and to address this the development of stable coins has been ongoing for the last few years. A stable coin is a cryptocurrency designed to mitigate volatility by being tied to an asset or grouping of assets. This asset can be either another cryptocurrency, fiat money, or any other tradeable commodity: this form of tying is called 'backed'. The relationship between the stablecoin and the backed commodity has to be pre-defined and pegged either on-chain via smart contracts, or off-chain through banks or financial institutions where the currency is located.

By market capitalization, Tether is the largest stablecoin with a market-cap of surpassing 18 billion USD[12] as of 2020. It has been put under scrutiny multiple times for not providing sufficient documentation of auditing, bringing into question the stated 1:1 backing ratio. A more complicated system, which has not yet been found at fault is Maker's DAI. The DAI is backed by collateral on the Maker platform which runs on Ethereum, executed by smart contracts, and attempts to maintain a value of 1 USD which, so far it, has successfully managed. It is founded on decentralized margin trading, facilitated by a Collateralized Debt Position (CDP): users deposit assets into smart contracts as collateral for loans. Once held by the CDP, the user can generate an equivalent amount of USD value in DAI and borrow it. This means the platform and thus the ratio-fixture is run by the users themselves and is highly transparent.

3.2 Corporate finance and governance

Public interest in blockchain technology is wider than in creating alternative monetary systems. The 2019 study on industry trends by Cambridge Centre for Alternative Finance (CCAF) has shown that 43% of enterprise blockchain networks used or being tested are in the Financial Services sector (Rauchs et al., 2019). This particularly includes already existent service providers experimenting with the technology; use cases extend to not only accounting but broader networks of interaction such as supply chain tracking, trading infrastructure, and document certification (Rauchs et al., 2019, p.10). The remaining percentage of blockchain systems known are spread across a wide range of sectors including government, media, manufacturing, energy, and health.

According to a report by the OECD (Akgiray, 2019), blockchain is meaningful for financial applications within the areas of capital markets, where the entire ecosystem can be modelled – payment systems, both cross-border and intra-national; OTC trading, a full trading cycle of bonds derivates, commodities, and other illiquid assets; and trade finance, where processes currently take several weeks and can be cut by circumventing intermediary steps, extra tasks and paperwork (Akgiray, 2019, p. 15). It is the capacity and ambition of the separate projects which set the limit for how far they can go, whether they end up using elements of blockchain technology or build entire infrastructures. The main choice lays with what sort of consensus the system will be based on, and whether this system will be multi-party or as a catalyst for process transformation. The first variant is where control across the network is shared and not centralized, allowing for collective agreement over data, whereas the second does not work with that aim, and instead use components of DLT technologies in order

to solve or potentially improve a business case. Unless a system is truly distributed, both in terms of data and authority, it remains an internal enterprise blockchain, with a pragmatic purpose rather than an idealistic one. A study of 67 enterprise blockchain systems revealed that only 3% were multi-party consensus networks, 20% had plans of becoming such, and the remaining 77% were using the system to reconfigure internal operations (Rauchs et al., 2019, p.19). This is not to say that internal systems have no impact; most new services and business models will come from such projects.

3.3 Financial accounting

Blockchain and DLT are ledger-based technologies, where distributed ledger constructs are being used to record transactions, and as such, they are by default an accounting methodology. Due to their decentralized and distributed nature, the creation, storage and updating of financial records is entirely changed. Through *universal entry bookkeeping* of sorts, every entry is shared identically and permanently with everyone participating. The key features which enable this are propagation, meaning *live* updating of the system, shared with everyone; permanence, determined by the consensus mechanism and allowing only for addition not editing; and programmability, essentially smart contract allowing for program code to be stored alongside transaction entries. Much of what accounting is concerned with is the measurement, sharing, and analysis of financial information. The goal is to ascertain or define ownership and duty or plan for the most beneficial way of allocating resources. Blockchain and DLT can be deployed to improve the entirety of the accounting profession by lowering the costs of keeping up and auditing ledgers, as the technology provides complete assurance of factuality. Instead of focusing on the recording process, accountants can use the improved clarity to concentrate on strategic decision-making and value estimation: blockchain would never take away the need for subjective decision-making. The scope can also be expanded by bringing in value from the measurement of previously unaccounted for data, such as proof of ownership.

It is not a new phenomenon that there is an effort to bring more transparency to accounting information. The organization International Financial Reporting Standards (IFRS, 2020) has been promoting trust and transparency to global financial markets and legislation against unlawful auditing has increased. Since the 1980s, triple-entry bookkeeping has been heralded as a new means for openness towards external users (Ijiri, 1986), whereby a third party can read a shared cryptographic receipt of a transaction between two parties. Since a 2014 article in Bitcoin Magazine (Tyra, 2014), the term has become synonymous with blockchain, and several projects have been created.

The most dominant actors in the accounting space are The Big Four accounting firms – Deloitte, PwC, EY, and KPMG – and all have been very active in R&D in the blockchain space the last couple of years, setting up teams like Deloitte's Rubix, FinTech strategy-consulting platforms such as PwC's Denovo, business applications like EY's Ops Chain, and partnerships with tech-providers such as KMPG's collaboration with Guardtime. Startups, smaller initiatives and research projects have also been developing enterprise blockchain solutions for the financial sector, and some noteworthy projects are zkLedger,[13] Pacio,[14] Request Network,[15] and Ledgerium.[16] To explain how blockchain and DLT based financial accounting works, we take the example of Ledgerium. Ledgerium is an Australian company founded in 2018, building a ledger Luca, which is a cloud-based platform recording payment transactions between parties via blockchain. The product is being partner tested, which means that some companies have cheap access to try out

the technology for their external auditing. How it works in practice is that company A needs to pay company B for a service done, and uses its accounting service, for example Xero, popular with Australians. The invoice is transmitted to Luca, with a hash and its details, and encrypted with the public key of company B. Company B will be notified of a request, and it can then verify and accept the transaction by requesting a hash. This is then added to the common ledger of the two parties, and Luca will automatically ping the bank to process the financial transaction, and add the payment after it has been completed. Auditors can then use the hashes of transactions or each party's actions to verify their truthfulness.

3.4 Financial reporting and compliance

When it comes to reporting and compliance there is a heightened focus on the legal quality of the accounting where the blockchain's aspect of immutability has always struck a promising chord. The two parts of the capital market confidence are transparency and monitoring. The transparency happens through the standards and regulations companies have to adhere to, and the monitoring happens by the regulating agencies which reinforce fairness. Blockchain helps both these processes, helping companies be more transparent and making monitoring easier. For example, in 2018 a US government guidance (ASC 606) stated exactly how revenue is recognized when it includes the use of contract, and companies which had been exploring smart contracts found it easier to comply as they had done exploratory work on products and services (Lewtan et al., 2018).

In light of regulations such as ASC 606, companies that use novel, and often more complex, business models will be able to more easily keep track of their revenue stream using blockchain-based services. As an example, video game publishers no longer focus on their point-of-sale/marketplace but rather on their end-users when it comes to creating long-term relationships: their games have deluxe versions in which extra content can be downloaded, currency and add-ons which can be used in-game, and continuous bug-fixes are all included. Users can also buy these things separately, at a higher price each. In a blockchain-setup, the end-user has a unique serial number, and the reseller can attach one upon sales. Sales will be linked back to the customer, but a token will be released by the smart contract with value price assigned which, after encryption onto the ledger, will show as revenue for the company. With downloaded updates, new content, or in-game currency, the tokens will be added, and even though the end-income shows as 'total sum', each new component will be traceable.

However, Molina-Jimenez et al. (2018b), in their exploratory paper on hybrid architectures for smart contract components, argue that both online and off-line systems have drawbacks: purely permission-less and truly democratic blockchain platforms lack scalability, speed, and are costly, among other limitations, whereas off-line systems require corruptible third parties. The smart contract acts as a service determining trust, transparency, throughput, response time, and cost, all depending on the type of operation taking place (e.g. rental or selling). No single type of uniform scenario exists, and each blockchain platform (e.g. Ethereum or Hyperledger) needs to be paired to the right off-line processing. In a Cambridge Computer Lab test, the team mimicked a hybrid model by using Rinkeby tenet of the Ethereum Blockchain for the on-blockchain component, and the Contract Compliance Checker tool for the off-line part (Molina-Jimenez et al., 2018a). These can read each other, and the result showed the architecture is implementable in case the off-blockchain component uses standard APIs able to communicate with the ones that blockchains use.

3.5 Crowdfunding, peer-to-peer lending and ICOs

In 2017, the digital equivalent of an Initial Public Offering (IPO), Initial Coin Offerings (ICOs) exploded, raising more than five billion USD in investments for crypto-based projects that year.[17] ICOs are decentralized fundraising initiatives for crypto-based projects. ICOs launch their tokens at a set price and the investors who are interested in these projects can buy these tokens using cryptocurrencies like Bitcoin (BTC) or Ether (ETH). Once sufficient tokens have been sold, the project is funded, can be started, built, and opened to holders of tokens to exchange these for services on the platform. Some platforms have a split between different tokens; some purely act as a currency, eligible for public exchange; others can be used for different services, or represent the value of different assets.[18]

As with any class of investment, particularly novel ones, most ICOs are not only very ambitious ("changing the game"), but actual scams, with no intent to realize project goals (Dowlat and Hodapp, 2018). ICOs obviously also have their benefits, as highly regulated crowdfunding-platforms can be avoided, smaller-scale initiatives can gather trusted support, creating value together, and sometimes very quickly. Some ICOs were suspended due to an overwhelming level of interest, such as Filecoin, Tezoz, and Brave (Adeyanju, 2017). The Brave browser was started by the former CEO of Mozilla Firefox, and is a decentralized web browser that gives users heightened data privacy and the opportunity to pay their most frequently used websites, encouraging an add-free internet; it raised 35 million USD in 30 seconds.[19] After China banned ICOs in late 2017, the market froze globally as heavy regulation was expected to follow, but recent offerings have slowly been picking up.

Any financially risk-averse entity rightfully awaits a reliable legal framework, and the European Securities and Markets Authority (ESMA) has only recently posted its advice (ESMA, 2019), concluding for instance "Because the range of crypto assets are diverse and many have hybrid features, ESMA believes that there is not a 'one size fits all' solution when it comes to legal qualification" (ESMA, 2019, p. 9). Tokens being judged on a case-by-case basis means that even after a launch, time has to be devoted to certification and approval. Today the cost for raising funds for a regulatory compliant ICO can be very high; an analysis by OECD[20] showed that conducting third-party security audits, communicating the benefits, and navigating other forms of requirements has costs ranging from between 50,000 and 500,000 USD. Despite this, projects that have emerged and continue to do so prove that the technology can help significantly support financial services through better workflow and management, contractual relationships and security (Weber, 2019). Crowdfunding mechanisms have also grown from ICOs and funnel investment into larger projects or a group of people, through their online platform systems. The project may be tied to financial gain (equity or interest) or non-financial rewards, or pure social impact. Examples of DLT representation in crowdfunding can be found in donation-based platforms (BlockBonds), match-funding (GOTEO), equity crowdfunding ecosystems (RealMarket), and more. New versions keep developing, like the 2018-founded platform WHIRL which is based on a "pay it forward" principle. Here a new project can only be initiated following active support of other projects by the founder(s), inspiring a perpetual loop of generosity and good reputation (Baber, 2019).

3.6 Derivative markets and smart contracts

As author Shermin Voshgmir puts it in the book *Token Economics* (Locklin, 2019) tokens are the most promising application of crypto-based technologies, and beyond ICOs there exist

security tokens. These represent security, a type of asset which is reliant upon or derived from, an underlying asset or group of assets such as stocks, bonds, interest rates, currencies etc. The asset and token are then interlinked via smart contracts, and these are tradeable financial instruments which can represent fractions of the total value of an asset. According to the European Securities and Markets Authority, security tokens can qualify as transferable securities under the MiFID directive, which has the role of protecting investors, but that the classification of each case is the role of the individual member states (ESMA, 2019, p. 4). The report highlights no disruption risk to traditional securities trading services, and even the European Central Bank has been exploring possible use-cases (ESMA, 2019).

Due to the way in which DLTs simplify the process of issuing, and reduce the duration of clearing and settlement, such processes can become simplified also on an institutional level. This is probably also where the largest success potential lies, in financial institutions taking up the securities to create liquidity in a decentralized way, skipping the step of fourth-party governance. It could lead to a significant lowering of cost for both investors and issuers, and therefore not just influence the transaction process but also the types of trading and exchanges that exist (EU Commission, 2019). Places where security exchanges and clearing houses have actively been testing blockchain-based models are national stock exchanges. In 2017 the Australian Stock Exchange (ASX) started planning the replacement of its widely recognized platform CHESS by blockchain technology from a startup named Digital Asset Holdings. The project is built on the open-source smart contract language DAML and was projected to be in deployment by 2019 but is still ongoing and with more collaboration partners. National stock exchange projects in Japan, Korea and India have been testing the technology for trading in low liquidity, shares of startups, and know-your-customer data protocols respectively (OECD, 2018). There are new experiments happening across many banks and exchanges, experimenting with things such as ways to make digital central bank-issued money available in trade and transaction of tokenized assets amongst different actors in the legacy systems (Swiss Stock Exchange and Swiss National Bank). These are currently still happening on an exploratory level, as the lack of stability and scalability of cryptocurrencies make it hard to reach large adoption. Further, formal regulation and legal adjustments in accordance with securities law are still catching up and leaving the situation in a precarious state.

4 Legal and regulatory perspectives of DLT

Blockchain-based technologies and DLTs have attracted significant attention from researchers in the law discipline, especially on aspects of regulation and governance of cryptocurrencies and blockchain-based applications such as smart contracts etc. The relevant extant literature research on the legal aspects of Blockchain regulation, compliance and governance is summarized in detail in Table 6.2.

As shown in Table 6.2, we can characterize the current research discussion on blockchain regulation into two distinct and opposing research streams: stringent regulation vs. open-minded regulation. First, the stream of research studies (Kleiman, 2013; Ajello, 2014; Lin, 2016) that is primarily concerned with money laundering and digital crime using cryptocurrencies and their economic and social impacts on societies, argues for establishing clear and stringent regulations, compliance protocols and guidance frameworks for the cryptocurrency industry. On the other hand, a significant amount of research (McLeod, 2014; Turpin, 2014; Kiviat, 2015; Sonderegger, 2015; Tsukerman, 2015; Colombo, 2016; Morgan, 2018; Priem, 2020) considers that blockchain is a highly disruptive and innovative technology and

Table 6.2 Research on regulatory initiatives of blockchain and DLTs

Article	*Primary theme*	*Main arguments and recommendations*
Kleiman (2013)	Regulation	Cryptocurrencies can be potential security and economic threats. Argues for establishing clear jurisdictional lines and regulations for the virtual currency industry.
Turpin (2014)	Regulation (favorable)	Argues for regulation, but is in favor of embracing the new technology. Recommends that governments should further study and regulate Bitcoin, but without attempting to stop or slow the growth of the currency itself and without attacking otherwise law-abiding citizens who transact in Bitcoins.
Ajello (2014)	Regulation, money laundering	Is concerned with Bitcoin's money laundering and its economic and social consequences. Advocates for more stringent regulations and argues that cryptocurrencies deserve greater attention from regulators and law enforcement officials.
McLeod (2014)	Regulation	Argues for regulation, but suggests amending the existing legal provisions in an amicable way to create a workable regulatory model for cryptocurrencies.
Sonderegger (2015)	Regulation (favorable)	Suggests that given Bitcoin's ideological and technological underpinnings, it requires a degree of regulatory freedom to succeed. Argues that proper regulation will not stifle innovation but will allow it to self-regulate within a vaguely defined regulatory framework.
Kiviat (2015)	Digital Assets, Regulation (favorable)	Argues that the true value of technology lies in its potential to facilitate more efficient digital-asset transfers and advocates that policymakers carefully define the specific activities that they seek to regulate.
Tsukerman (2015)	Regulation (favorable)	Claims that unmasking actors on the blockchain will help Bitcoin shed its infamous reputation and that Bitcoins must be brought into the light and seen as a useful currency, and not simply as the refuge of dark web inhabitants.
Colombo (2016)	Regulation (favorable)	Argues that responsibility of regulators and lawmakers is to establish rules that safeguard consumers and markets without hindering growth and innovation. Opines that it will be difficult to get right when dealing with something as new and alien (to fiat currency regulatory apparatus) as virtual currency.
Lin (2016)	Cybersecurity, compliance	Focuses on the challenges of financial cybersecurity, technology integration, compliance, and the role of humans in the future of modern finance.
Lee (2016)	Cyber securities and stock markets	Argues that blockchain will create crypto securities that will allow the public to verify transactions if they want, which will remove some of the hidden secrecy surrounding much of the high frequency and dark pool trading occurring today.
Gabison (2016)	Regulation, accountability	Argues for the need for policymakers to reinvestigate several laws and rights for blockchain. Fears that lack of accountability to a policing authority exposes users to attacks and allows potential transfers that finance criminal activities.
Christopher (2016)	Enforcement and trust	Argues that Bitcoin requires more trust than is generally understood and both currency and payment systems benefit from the involvement of trusted intermediaries in response to problems and crises.

(*Continued*)

Article	*Primary theme*	*Main arguments and recommendations*
Rosner and Kang (2016)	Flexible regulation	Argues for a flexible and principles-based approach to amend current regulatory frameworks to account for modern technological realities. Claims that the cryptocurrency Ripple's advantages suggest that users will increasingly use these systems in place of traditional payment. processes.
Shackelford and Myers (2017)	Cyber security, regulation	Examines blockchains through the lens of polycentric governance to ascertain what could be done to build trust in distributed systems and ultimately promote cyber peace. Assess that it will take many years to build sustainable blockchain system by involving numerous stakeholders and policymakers.
Guo (2017)	Patents for blockchain technology	Discusses whether trade secret or copyright protection should apply to protect the claims and uses of blockchain technology and states that only time will tell if blockchain technology can be claimed as intellectual property or be used in court.
Reyes (2017)	Crypto-legal structures	Advocates for usage of blockchain technologies for legal systems (crypto law) and argues that crypto law could offer a legal discourse to serve more rapidly, more efficiently, more transparently, and in creative ways, that may encourage increased civic engagement.
Ross (2017)	Regulation, National charter	Claims that regulatory emphasis on the threat posed by cryptocurrencies has created a hostile environment to innovation. Advises establishing a national charter for FinTech to absorb the full potential of blockchain technology.
Surujnath (2017)	Derivatives markets	Advocates that blockchains with self-executing smart-contracts provide compelling opportunities in derivatives markets and that they can reduce dependency on central counterparties that are exposed to large amounts of credit risk.
Sklaroff (2017)	Smart vs semantic contracts	Argues that semantic contracts offer two forms of flexibility: linguistic ambiguity and enforcement discretion, which are important in the contracting process and therefore smart contracting will impose more costs than semantic contracts.
Arrun˜ada (2018)	Smart contracts for property rights	Argues that intermediaries' role is crucial in the processes of firms' strategies and contracting and therefore cannot be replaced by blockchain but argues for private blockchains for archiving purposes within standard registration systems.
Morgan (2018)	Open-minded regulation	Argues for the regulation of cryptocurrencies with a more open-minded approach to promote truly informed policy decisions as opposed to irrational and poor investment decisions.
Young (2018)	Smart constitution, smart social contract	Advocates for a smart constitution, to make the government operate transparently and within its mandate; also argues that "When something is codified, and connected to the blockchain, *code is law.* When the code is the law, any entity tied to it is powerless to act outside of the code. This will ensure that governments stay within their expressed powers." Young (p.71, 2018).
Suciu et al. (2019)	Regulation for crypto-based businesses	Explores the initiatives for the regulation of crypto-based businesses such as ICOs in the UK, Estonia and Switzerland; posits that these are friendly companies when it comes to doing digital businesses.

Article	*Primary theme*	*Main arguments and recommendations*
(Franks, 2020)	Records management	Presents several opportunities and challenges in terms of using DLT for records management and information governance.
(Priem, 2020)	Policy debate on regulation of DLTs	Explores which regulatory barriers need to be removed for full adoption of DLTs; identifies the challenges and risks related to DLT systems; provides a good summary of the regulatory initiatives in EU for DLTs.

argues for a more open-minded regulation without attempting to stop or slow its growth with suggestions to amend the existing legal provisions if necessary to create a workable regulatory model. Moreover, it is argued that a proper regulatory model that does not constrain the innovation of cryptocurrencies will allow them to self-regulate within a vaguely defined regulatory framework; at the same time revealing the identities of the actors in case of necessities (e.g. money laundering) will help the cryptocurrencies to get rid of their infamous reputation and potentially revolutionize organizations.

Apart from cryptocurrencies such as Bitcoin, prior research also focused on the regulation and compliance in terms of using blockchain and DLTs for various applications such as digital-asset transfers (Kiviat, 2015), property rights (Arrun˜ada, 2018), crypto securities (Lee, 2016), derivatives markets (Surujnath, 2017), smart contracts (Sklaroff, 2017), records management (Franks, 2020) and so on for financial, accounting and other administrative domains. Unlike the case of cryptocurrencies, the research from the law disciplines has argued for the usage of blockchain technology for developing applications in these areas, as it would enhance transparency by removing hidden secrecy and provide a way for more efficient document and authorship verification, title transfers, and contract enforcement. Finally, just to provide an example of the scope of research regarding blockchain regulation and governance Young (2018) advocated for a smart constitution, a blockchain-based implementation for governance, which would make government operate in compliance with smart constitution laws visibly and would also prohibit it from operating outside of its mandate. Given that this extensive discussion on regulation and compliance is important for trusted third-party providers, it is apparent that governmental agencies or regulators need to implement flexible regulatory and compliance measures for cryptocurrencies without burdening law-abiding citizens who transact with cryptocurrencies and DLTs within the legal framework.

5 Conclusion

In this book chapter, we discussed various principles and concepts behind the DLT and blockchain technologies such as hash functions, digital signatures and digital timestamping which form the foundations of the DLTs and blockchains. We have also introduced how various consensus protocols and fault tolerance mechanisms can help to achieve consensus in a distributed and decentralized environment like blockchain and DLTs. In addition to that, a detailed description of how DLT and blockchain applications can impact the FinTech applications is also provided. We also summarized the existing research and initiatives in terms of legal and regulatory perspectives on DLT and blockchain.

5.1 Regulation

For the last few years, there has been a growing demand for regulatory measures on blockchain applications, especially for cryptocurrencies. Since cryptocurrencies employ a high level of anonymity (Sun Yin et al., 2019), they have been labelled as the go-to currencies for illicit activity. The shutdown of the drug market Silk Road provides the most well-known example (Christin, 2013). Moreover, recent articles and reports (Hout and Bingham, 2013; Martin, 2014a; Martin, 2014b) have stated that Bitcoin has been used for terror financing, thefts, scams, and ransomware. Financial regulators, law enforcement, intelligence services, and companies who transact on the Bitcoin blockchain have become wary observers of technical developments in Bitcoin, economic issues with it, and the societal implications of its adoption (Ali et al., 2015; B¨ohme et al., 2015). In light of these developments, there has been a great demand for regulatory measures to be put in place to control the illicit activities associated with cryptocurrencies and other blockchain applications. Although there has been no specific regulation adopted for cryptocurrencies and blockchain applications, there have been several initiatives (Financial Conduct Authority, 2017; Financial Stability Board, 2018) to examine the need for new regulation or whether to modify existing regulation in order to harness the full potential of blockchain technology. However, many regulatory authorities are still monitoring the rapid growth of these technologies and their influence on FinTech applications. As discussed in the previous section, many regulators and legal authorities still think that blockchain technology is in its infancy stage although evolving at a fast rate, and that it will be necessary to study challenges and barriers in a much more thorough way before putting in place a regulatory framework for DLT and blockchain applications.

5.2 Market adoption

Technological advancements are a necessary but not sufficient condition for the widespread market adoption of DLT-based FinTech products and services. Advancements in DLT are necessary to address the known critical issues of low transaction volume, energy inefficiencies, and regulatory challenges in terms of cybersecurity vulnerabilities and cybercriminal activities. That said, technological advancements in DLT are not sufficient as established players and entrenched interests still experience favorable market conditions such as highly standardized terms and inter-institutional operations.

In conclusion, technological advancements in DLT intertwined with service innovations will continue to play an influential role in the evolution of FinTech in the near future.

Notes

1 https://coinmarketcap.com/
2 https://www.statista.com/statistics/730876/cryptocurrency-maket-value/
3 https://www.eublockchainforum.eu/eu-blockchain-observatory-forum
4 https://coinmarketcap.com/
5 http://www.weidai.com/bmoney.txt
6 https://unenumerated.blogspot.com/2005/12/bit-gold.html
7 https://coinmarketcap.com/
8 https://smartdec.net/
9 https://openzeppelin.com/
10 https://chainsecurity.com/
11 https://starkware.co/
12 https://cryptoslate.com/cryptos/stablecoin/

13 https://dci.mit.edu/zkledger
14 https://pacio.io/
15 https://request.network/en/
16 https://www.ledgerium.io/
17 https://amp.insider.com/how-much-raised-icos-2017-tokendata-2017-2018-1
18 https://treehouse.online/static/whitepaper/treehouse-whitepaper.pdf
19 https://techcrunch.com/2017/06/01/brave-ico-35-million-30-seconds-brendan-eich/
20 https://www.oecd.org/daf/ca/The-Potential-for-Blockchain-in-Public-Equity-Markets-in-Asia.pdf

References

Adeyanju, Craig (2017) How a loyalty program on blockchain works, explained, December. https://cointelegraph.com/explained/how-a-loyalty-program-on-blockchain-works-explained

Ajello, Nicholas J. (2014) Fitting a square peg in a round hole: Bitcoin, money laundering, and the fifth amendment privilege against self-incrimination. *Brooklyn Law Review*, 80(2): 435.

Akgiray, Vedat (2019) The potential for blockchain technology in corporate governance. Technical report, OECD Corporate Governance Working Papers.

Ali, Syed Taha, Dylan Clarke and Patrick McCorry (2015) Bitcoin: Perils of an unregulated global p2p currency. In *Cambridge International Workshop on Security Protocols*. Springer.

Antonopoulos, Andreas M. (2014) *Mastering Bitcoin: unlocking digital cryptocurrencies*. O'Reilly Media, Inc.

Arruñada, Benito (2018) Blockchain's struggle to deliver impersonal exchange. *Minnesota Journal of Law, Science & Technology*, 19(1): 55.

Baber, Hasnan (2019) Blockchain-based crowdfunding: A 'pay-it-forward'model of whirl. *International Journal of Recent Technology and Engineering (IJRTE)*, 8(3): 2277–3878.

Back, Adam (2002) Hashcash-a denial of service counter-measure. http://www.hashcash.org/papers/hashcash.pdf.

Bayer, Dave, Stuart Haber and W. Scott Stornetta (1993) Improving the efficiency and reliability of digital time-stamping. In *Sequences Ii*. Springer, pp. 329–334.

Ben-Sasson, Eli, Iddo Bentov, Yinon Horesh and Michael Riabzev (2019) Scalable zero knowledge with no trusted setup. In *Annual International Cryptology Conference*. Springer, pp. 701–732.

Böhme, Rainer, Nicolas Christin, Benjamin Edelman and Tyler Moore (2015) Bitcoin: Economics, technology, and governance. *The Journal of Economic Perspectives*, 29(2): 213–238.

Carter, J. Lawrence and Mark N. Wegman (1979) Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2): 143–154. ISSN 0022-0000. http://www.sciencedirect.com/science/article/pii/0022000079900448.

Castro, Miguel Barbara Liskov, et al. (1999) Practical byzantine fault tolerance. *OSDI*, 99: 173–186.

Chohan, Usman W. (2017) A history of bitcoin. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047875.

Christin, Nicolas (2013) Traveling the silk road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd International Conference on World Wide Web*, WWW. New York, NY, USA, pp. 213–224. ACM. ISBN 978-1-4503-2035-1.

Christopher, Catherine Martin (2016) The bridging model: Exploring the roles of trust and enforcement in banking, bitcoin, and the blockchain. *Nevada Law Journal*, 17: 139.

Colombo, Ronald J. (2016) Bitcoin: Hype or harbinger. *Journal of International Business and Law*, 16(1): 1.

Dalvit, Lorenzo (2020) Ethereum: A new record of transactions per second thanks to Istanbul, January. https://en.cryptonomist.ch/2020/01/07/ethereum-transactions-per-second-istanbul/.

Damård, Ivan Bjerre (1989) A design principle for hash functions. In *Conference on the Theory and Application of Cryptology*. Springer, pp. 416–427.

Dowlat, Sherwin and Michael Hodapp (2018) Ico quality: Development and trading, March. https://www.bitcoininsider.org/article/21901/ico-quality-development-trading.

Dworkin, Morris J. (2015) *Sha-3 standard: Permutation-based hash and extendable-output functions*. Technical report, National Institute of Standards and Technology (NIST).

ESMA (2019) Advice, initial coin offerings and crypto-assets. Technical report, European Securities and Markets Authority.

European Central Bank (2012) *Virtual currency schemes*. Frankfurt am Main, Germany.
European Central Bank (2015) *Virtual currency schemes: A further analysis*. Technical report, Frankfurt am Main, Germany.
EU Commission (2019) *Potential use cases for innovative technologies in securities post-trading*. Technical report, European Central Bank.
Faber, Benedict, Georg Cappelen Michelet, Niklas Weidmann, Raghava Rao Mukkamala, and Ravi Vatrapu (2019) Bpdims: A blockchain-based personal data and identity management system. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.
Financial Conduct Authority (2017) Discussion paper on distributed ledger technology. Technical report, Financial Conduct Authority.
Financial Stability Board (2018) *Crypto-assets: Report to the g20 on the work of the fsb and standardsetting bodies*. Technical report, Financial Stability Board, Basel, Switzerland.
Franks, Patricia C. (2020) Implications of blockchain distributed ledger technology for records management and information governance programs. *Records Management Journal*.
Gabison, Garry (2016) Policy considerations for the blockchain technology public and private applications. *Science and Technology Law Review*, 19: 327.
Goldwasser, Shafi, Silvio Micali, and Charles Rackoff (1989) The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1): 186–208.
Guo, Angela (2017) Blockchain receipts: Patentability and admissibility in court. *Chicago–Kent Journal of Intellectual Property*, 16(2): 440.
Haber, Stuart and W. Scott Stornetta (1990) How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography*. Springer, pp. 437–455.
Heilman, Ethan, Neha Narula, Garrett Tanzer, James Lovejoy, Michael Colavita, Madars Virza, and Tadge Dryja (2019) Cryptanalysis of Curl-P and other attacks on the IOTA cryptocurrency. *IACR Cryptol. ePrint Arch.*: 344. https://eprint.iacr.org/2019/344.pdf.
Hout, Marie Claire Van and Tim Bingham (2013) Silk road, the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy*, 24 (5): 385–391. ISSN 0955–3959. http://www.sciencedirect.com/ science/article/pii/S0955395913000066.
IFRS (2020) List of IFRS Standards, September. https://www.ifrs.org/issued-standards/list-of-standards/.
Ijiri, Yuji (1986) A framework for triple-entry bookkeeping. *Accounting Review*, 745–759.
Johnson, Don, Alfred Menezes and Scott Vanstone (2001) The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*, 1(1): 36–63.
Kiviat, Trevor I. (2015) Beyond bitcoin: Issues in regulating blockchain tranactions. *Duke Law Journal*, 65: 569.
Kleiman, Jared A. (2013) Beyond the silk road: Unregulated decentralized virtual currencies continue to endanger US national security and welfare. *American University National Security Law Brief*, 4(1): 59.
Lamport, Leslie (2019) The part-time parliament. In *Concurrency: the Works of Leslie Lamport*, pp. 277–317. ACM Books.
Lamport, Leslie, Robert Shostak and Marshall Pease (1982) The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3): 382–401.
Lamport, Leslie et al. (2001) Paxos made simple. *ACM Sigact News*, 32(4): 18–25.
Lee, Larissa (2016) New kids on the blockchain: How bitcoin's technology could reinvent the stock market. *Hastings Business Law Journal*, 12(2): 81.
Lewtan, Jacob, Joseph McManus and Saeed Roohani (2018) Blockchain: Opportunity to improve financial reporting and corporate governance. In *Hawai'i Accounting Research Conference (HARC)*.
Lin, Tom C.W. (2016) Compliance, technology, and modern finance. *Brooklyn Journal of Corporate, Financial and Commercial Law*, 11(1): 159.
Locklin, Scott (2019) *Token economics*. Technical report, Brave Software.
Mamoshina, Polina, Lucy Ojomoko, Yury Yanovich, Alex Ostrovski, Alex Botezatu, Pavel Prikhodko, Eugene Izumchenko, Alexander Aliper, Konstantin Romantsov, Alexander Zhebrak, et al. (2018) Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget*, 9(5): 5665.
Martin, James (2014a) *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Springer.
Martin, James (2014b) Lost on the silk road: Online drug distribution and the cryptomarket. *Criminology & Criminal Justice*, 14(3): 351–367. http://dx.doi.org/10.1177/1748895813505234.

McLeod, Patrick (2014) Taxing and regulating bitcoin: The government's game of catch up. *CommLaw Conspectus*, 22: 379.

Merkle, Ralph C. (1980) Protocols for public key cryptosystems. In *Security and Privacy, 1980 IEEE Symposium on*, pp. 122–122. IEEE.

Merkle, Ralph C. (1989) One way hash functions and DES. In *Conference on the Theory and Application of Cryptology*, pp. 428–446. Springer.

Molina-Jimenez, Carlos, Ioannis Sfyrakis, Ellis Solaiman, Irene Ng, Meng Weng Wong, Alexis Chun and Jon Crowcroft (2018a) Implementation of smart contracts using hybrid architectures with on and off–blockchain components. In *2018 IEEE 8th International Symposium on Cloud and Service Computing (SC2)*, pp. 83–90. IEEE.

Molina-Jimenez, Carlos, Ellis Solaiman, Ioannis Sfyrakis, Irene Ng, and Jon Crowcroft (2018b) On and off-blockchain enforcement of smart contracts. In *European Conference on Parallel Processing*, pp. 342–354. Springer.

Morgan, Joshua S. (2018) What I learned trading cryptocurrencies while studying the law. *University of Miami International and Comparative Law Review*, 25:159.

Nakamoto. Satoshi (2008) *Bitcoin: A peer-to-peer electronic cash system*. [White Paper] https://bitcoin.org/bitcoin.pdf.

Narayanan, Arvind and Jeremy Clark (2017a) Bitcoin's academic pedigree. *Communications of the ACM*, 60(12):36–45, November. https://doi.org/10.1145% 2F3132259.

Narayanan, Arvind and Jeremy Clark (2017b) Bitcoin's academic pedigree. *Communications of the ACM*, 60(12): 36–45.

Natarajan, Harish, Solvej Karla Krause and Helen Luskin Gradstein (2019) Distributed ledger technology (DLT) and blockchain. Fintech note; no. 1. Washington, DC: World Bank Group.

OECD (2018) *The potential for blockchain technology in public equity markets in Asia*. Technical report, OECD Capital Market Series.

Penard, Wouter and Tim van Werkhoven (2008) On the secure hash algorithm family. *Cryptography in Context*, pp. 1–18.

Priem, Randy (2020) Distributed ledger technology for securities clearing and settlement: Benefits, risks, and regulatory implications. *Financial Innovation*, 6(1): 1–25.

Rauchs, Michel, Andrew Glidden, Brian Gordon, Gina C Pieters, Martino Recanatini, Francois Rostand, Kathryn Vagneur, and Bryan Zheng Zhang (2018) Distributed ledger technology systems: A conceptual framework. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230013.

Rauchs, Michel, Apolline Blandin, Keith Bear, and Stephen B. McKeon (2019) *Second global enterprise blockchain benchmarking study*. Technical report, Cambridge Centre for Alternative Finance (CCAF).

Reyes, Carla L. (2017) Conceptualizing cryptolaw. *Nebraska Law Review*, 96(2): 384.

Rivest, Ronald L., Adi Shamir, and Len Adleman (1978) A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2): 120–126.

Rosner, Marcel T. and Andrew Kang (2016) Understanding and regulating twenty-first century payment systems: The ripple case study. *Michigan Law Review*, 114(4): 649.

Ross, Elizabeth Sara (2017) Nobody puts blockchain in a corner: The disruptive role of blockchain technology in the financial services industry and current regulatory is- sues. *Catholic University Journal of Law and Technology*, 25(2): 7.

Shackelford, Scott J. and Steve Myers (2017) Block-by-block: Leveraging the power of blockchain technology to build trust and promote cyber peace. *Yale Journal of Law and Technology*, 19(1): 334.

Simmons, Gustavus J. (1994) *Contemporary cryptology: The science of information integrity*. IEEE Press.

Sklaroff, Jeremy M. (2017) Smart contracts and the cost of inflexibility. *University of Pennsylvania Law Review*, 166: 263.

Sonderegger, Daniela (2015) A regulatory and economic perplexity: Bitcoin needs just a bit of regulation. *Washington University Journal of Law & Policy*, 47: 175.

Suciu, Christina Marta, Christian Nasulea and Diana Florentina Nasulea (2019) To- wards developing a friendlier regulatory framework for blockchain-based businesses. *Economic Convergence in European Union*, p. 15.

Sun Yin, Hao Hua, Klaus Langenheldt, Mikkel Harlev, Raghava Rao Mukkamala and Ravi Vatrapu (2019) Regulating cryptocurrencies: A supervised machine learning approach to de-anonymizing the bitcoin blockchain. *Journal of Management Information Systems*, 36(1): 37–73.

Surujnath, Ryan (2017) Off the chain: A guide to blockchain derivatives markets and the implications on systemic risk. *Fordham Journal of Corporate & Financial Law*, 22 (2): 257.

Swan, Melanie (2015) *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.
Szabo, Nick (1997) Formalizing and securing relationships on public networks. *First Monday*, 2(9), Sept. ISSN 1396–0466. http://dx.doi.org/10.5210/fm.v2i9.548.
Szostek, Dariusz (2019) *Blockchain and the Law*. Nomos Verlag.
Treleaven, Philip, Richard Gendal Brown, and Danny Yang (2017) Blockchain technology in finance. *Computer*, 50(9): 14–17.
Tsukerman, Misha (2015) The block is hot: A survey of the state of bitcoin regulation and suggestions for the future. *Berkeley Technology Law Journal*, 30(4): 1127.
Turpin, Jonathan B. (2014) Bitcoin: The economic case for a global, virtual currency operating in an unexplored legal framework. *Indiana Journal of Global Legal Studies*, 21(1): 335–368.
Tyra, Jason M. (2014) Triple entry bookkeeping with bitcoin, February. https://bitcoinmagazine.com/articles/triple-entry-bookkeeping-bitcoin-1392069656.
Wang, Wenbo, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim (2019) A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access*, 7: 22328–22370.
Weber, Conny (2019) *Exploring DLT and blockchain for alternative finance: A collection of case studies*. Technical report, European Crowdfunding Network, November.
Xu, Lihao (1999) *Highly available distributed storage systems*. PhD thesis, California Institute of Technology.
Young, Steve (2018) Enforcing constitutional rights through computer code. *Catholic University Journal of Law and Technology*, 26(1): 1.