Chapter 1

Cryptocurrencies: Concept and Current Market Structure

**Octavian Nica^{*,†}, Karolina Piotrowska^{*,§},
and Klaus Reiner Schenk-Hoppé^{*,†,¶}**

^{}Economics, School of Social Sciences, University of Manchester, UK*

*[†]Department of Finance, NHH — Norwegian School of Economics,
Bergen, Norway*

[‡]octavian.nica.96@gmail.com

[§]kk.piotrowska@cjbs.net

[¶]klaus.schenk-hoppe@manchester.ac.uk

Abstract

Since the creation of Bitcoin in 2009, hundreds of cryptocurrencies have emerged, thus becoming a common fixture of financial news bulletins. With a market capitalization of the five highest-valued cryptocurrencies exceeding \$140 billion at the time of writing, these alternative currencies have caught the attention of both financial institutions and central banks with their innovative technological foundations and their potential to disrupt current financial institutional structures. We provide a non-technical overview of the concept and current market structure of cryptocurrencies for researchers in economics, finance, mathematics and computer science.

Keywords: introduction to cryptocurrencies, blockchain, mining, governance

1. A Brief History of Cryptocurrencies

Cryptocurrencies are generally characterized in the academic literature as a subtype of alternative currencies (Hileman, 2014; Nian and Kuo Chuen, 2015; Wood and Buchanan, 2015). Alternative currencies — “*any medium of exchange other than legal tender*” (Hileman, 2014, p. 7) — are not a new concept, as they have recurrently been present over the last few centuries, sometimes bearing a significant role in the economy (Hileman, 2014). What differentiates cryptocurrencies from any other alternative currency (or digital currency, for that matter) is that they are a medium of exchange that, in its purest form, does not require any central authority that accomplishes transactions or manages the currency supply. This level of decentralization is made possible through the use of cryptography. Cryptography can be used for two general purposes. The first one is to conceal (or partially conceal) the identity of participants in the market. The second use of cryptography is to require participants to solve a cryptographic puzzle. By solving the puzzle, users collectively validate the transactions that occur on the market, thus making safe transactions in the currency without the need of oversight from a trusted third party agent, and also receive units of currency as a reward, thus establishing a rule for the creation of currency (Nian and Chuen, 2015). Since 2009, the number of cryptocurrencies has surged, and many of them have moved away from this pure model.

1.1 *The Precursors of Bitcoin*

The idea of a cryptocurrency first appeared in Chaum (1982), who was motivated in his endeavor by the fact that electronic payment systems could impact personal privacy (Chaum, 1982). His solution to these issues was a “blind signatures cryptosystem,” a system where cryptographic functions are used to conceal the identity of the payers and payees, while offering them the possibility to verify if the transaction has been completed. In a subsequent paper, Chaum introduced the concepts of “electronic wallets,” and “public and private signatures” (Chaum, 1983), which are two ideas that are fundamental to cryptocurrencies in use today. Thus, Chaum created the first digital currency that made use of cryptography, called eCash, in 1990. Unlike most cryptocurrencies today, eCash was a centralized currency and it used cryptography to conceal the identity of users (Nian and Chuen, 2015).

In the 1990s and early 2000s, cryptocurrencies continued to be of academic interest. Szabo (1998, 2002) published extensively on the concept of money and devised a concept of cryptocurrency in Szabo (2008) just before the appearance of Bitcoin. In 1991, Haber and Stornetta (1991) introduced the idea of a blockchain that uses timestamping to authenticate authorship of intellectual property. Dwork (2006) and Back (2002) created a cryptographic proof-of-work algorithm called Hashcash which, even though not initially conceived for cryptocurrencies, later became the cryptographic puzzle used in many currencies, including Bitcoin, to allow networks of users to verify transactions in a decentralized manner.

In parallel, the technology behind Internet payments improved with the emergence of a series of digital currencies based on gold. These currencies were essentially asset-backed payment systems (Nian and Chuen, 2015). Of these gold standard digital currencies, the most popular was e-gold which, before its closure in 2008, was processing more than \$2 billion per year. E-gold's popularity decreased as the currencies faced attacks from hackers and cases of Internet fraud, and it was shut down as it did not comply with the legal requirements imposed by US authorities.

1.2 *The Emergence of Bitcoin*

Bitcoin appeared in 2008, when an anonymous group, working under the pseudonym of Satoshi Nakamoto, published a whitepaper detailing the design of the currency (Nakamoto, 2008). Bitcoin is the first fully decentralized currency, and it can be operated by anyone who downloads its open-source software. This means that the currency is essentially a peer-to-peer network where all the users are connected with each other and can make transactions without the need for any third party, such as a bank. Bitcoin uses public-key cryptography in order to make transactions computationally impractical to reverse, thus, in theory, protecting users from fraud and preventing double spending. The supply of currency is determined by a predefined algorithm and new currency is released through a process of "mining," which means that certain users are rewarded with new currency units for performing computationally intensive tasks that are necessary for the Bitcoin system to function. Mining rewards stop after a ceiling of 21 million bitcoins is reached. From this point forward, Nakamoto (2008) argues that transaction fees can become a sufficient incentive for miners to keep performing their work.

After publishing the 2008 paper, Nakamoto (2009) popularized the new currency on online forums and mined the genesis block of Bitcoin in the same year, but Bitcoin remained a fringe phenomenon until about 2011. At that time, the currency suddenly gained traction, helped in part by the decision of Mt. Gox, a Japanese-based exchange for fantasy games cards, to allow trading in Bitcoins (Yermack, 2015). The sudden growth of cryptocurrencies from 2011 onwards can also be explained by the fact that Bitcoin was the first online currency to publish its entire source code online and—allow for it to be used and modified freely.¹ This has fostered the creation of alternative currencies based on its code. Some of these new currencies exist totally separated from the Bitcoin environment, having their own genesis block, while others are simply branches of the blockchain of Bitcoin. By the end of 2011, Tarasiewicz and Newman (2015, p. 202) reported that there were already 10 alternative cryptocurrencies in use, while at the end of 2013 the number of alternative currencies reached 215.

There are different reasons that explain the sudden rise in interests for cryptocurrencies. Hileman (2014, p. 164) presents a list of these reasons, mentioning, among others, the following: inefficiencies in the current financial system (long waiting times for transactions, high transaction fees), disbelief in the current political system (especially in the relations between the government and large financial institutions), technological innovations (cryptographic advances, increase in computational power) and speculation.

Among these diverse driving forces, the one that received the most attention in academic publications and in the media is the political foundation of the cryptocurrency movement. From its inception, the cryptocurrency community was associated with libertarianism (Huckle and White, 2016; Ametrano, 2016). A survey conducted in 2014 on the Bitcoin community shows that almost 60% of the respondents self-identify as libertarians, whereas 27% of them define themselves as anarchists (Lustig and Nardi, 2015, p. 9). Gavin Wood, one of the founders of Ethereum, another popular cryptocurrency initiative, is critical of the role of both the government and banks, arguing, in a paper, for the “*decentralisation of authority*” (Wood and Buchanan, 2015, p. 387) in the financial system.

¹The Bitcoin source code is currently available from its Github repository at <https://github.com/bitcoin/bitcoin>.

Nakamoto himself shares the same view with the libertarian community when it comes to economic matters:

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. (Nakamoto, 2009)

The political foundations of Bitcoin are reflected in the way its currency supply is managed. The fact that the creation of new currency works according to an unalterable algorithm, which is only an intermediary phase until the 21 million bitcoins limit is reached, can be partially explained through the anti-central banks rhetoric that criticizes the system of centralized fiat currencies that has been in place since the complete abolishment of the gold standard in 1971 (Golumbia, 2016).

The increased popularity of Bitcoin is also attributed to its adoption as a preferred payment method by Silk Road, which was the biggest online marketplace for drugs and other illegal goods and services. It based its existence on Tor, a software that allows users to browse the Web without the possibility of being tracked, and Bitcoin, which allowed for anonymous payments. Christin (2012, p. 20) estimated that in 2013 between 4.5 and 9% of all Bitcoin exchange trades were related to Silk Road. In 2013, the website was shut down by the Federal Bureau of Investigations, but it is estimated that the sites that replaced it soon became larger than Silk Road (Soska and Christin, 2015). Bitcoin's popularity suffered when Mt. Gox, the first exchange for Bitcoin (that also became the largest one, handling around 80% of all the transactions), closed down and filed for bankruptcy protection in 2014 (Abrams and Popper, 2014). The company lost almost 850,000 bitcoins (which, at that time, amounted to around \$450 million), and its CEO was arrested and charged with fraud and embezzlement.

Since 2014, the general perception of cryptocurrencies has become more positive. According to De Filippi and Loveluck (2016), this is mostly due to Bitcoin bringing a new opportunity for speculation. This increase in Bitcoin's popularity led to the creation of a new variety of cryptocurrencies that moved away from the political and ideological

ideas behind Bitcoin. These new currencies are more likely to embrace the centralization of certain parts of their infrastructure and accept more conventional governance structures. These factors made financial institutions embrace cryptocurrencies on a larger scale: The New York Stock Exchange, Goldman Sachs and BBVA have invested in cryptocurrency start-ups (Shin, 2015) and both a Wall Street clearinghouse and the Australian Securities Exchange announced that they are planning on adopting blockchain technology (Popper, 2017; Yermack, 2017).

Financial institutions are not necessarily interested in cryptocurrencies but in the blockchain technology. For instance, Hyperledger — one of the largest consortia of companies that decided to invest in blockchain technology — made clear that they will never be interested in creating a new currency.² The prospect for an even bigger increase in the cryptocurrency market is given by the new funding mechanisms for innovations, called Initial Coin Offerings (ICOs). An ICO, which is a method that is somewhere between a traditional Initial Public Offering (IPO) and a crowd-funding initiative, gives investors early access to new coins in return for investment funds (Kaminska and Murphy, 2017).

Most of the new cryptocurrencies not only work as currencies but also fulfill other auxiliary roles. Ripple, for instance, is a cryptocurrency project that also creates a currency exchange and remittance network which is based on the blockchain technology. Another popular cryptocurrency project, Ethereum, with its own currency called Ether, realizes Szabo's idea of "smart contracts" (Szabo, 1997). These are self-enforcing contracts that work through blockchain technology.

The close links between conventional financial institutions and the cryptocurrency community have deepened the division that already existed in the latter between a core group of supporters of a more idealistic version of cryptocurrencies and a group of users that see cryptocurrencies as the sign of a new, emerging technology or just as an investment opportunity. This division can be seen in the various governance crises, when the inability of the community to reach a consensus puts currencies like Bitcoin (Popper, 2016), Ethereum (Coppola, 2016) or Litecoin at the risk of breaking apart.

²<http://www.eweek.com/cloud/hyperledger-blockchain-project-is-not-about-bitcoin>.

2. The Mechanisms Behind Cryptocurrencies

The cryptographic nature of the underlying mechanism which enables the decentralization of cryptocurrencies is the main technological feature distinguishing them from other digital currencies. As a result, Bitcoin has become the first currency which allows the transfer of money without the mediation of a third party (Franco, 2014).

2.1 Transaction Path and Wallets

We define cryptocurrency as a *fixed-value cryptographic object represented as a chain of digital signatures over the transactions in which the coin was used* (Kroll *et al.*, 2013). A chain of digital signatures is a data pattern the digital value is assigned to. What distinguishes it from any other worthless stream of data is the fact that its system prevents *double spending* without the involvement of a central counterparty. This is possible thanks to the introduction of the *blockchain*, a public ledger that is the common element of different cryptocurrency systems.

In contrast to a central authority system, information about the balance of the user's account is available to everyone. Users are identified by large strings of characters known as *addresses*. These are the public part of the public-private cryptographic keys. The private piece, a *signature*, is controlled only by the user. As a result of excluding any third party from the system and identifying participants only by their addresses, their pseudo-anonymity is preserved.

When one participant sends some tokens to another user, she advertises the message stating that a given amount of coins is supposed to be subtracted from her address and added to another one. The new transaction generates a hash, which provides the details of the message and points to the previous transaction the coin was used in.

As a result, every token can be traced back to its inception. Subsequently, a user signs the message with a *digital signature* — a code that is cryptographically derived from the message and private key. Such a transaction is sent to the network. Upon receiving the message, there are three steps that must be completed before the transaction is finalized (Franco, 2014). Firstly, the signature is verified. Next, the balance of the sending address account is checked in order to determine whether there are sufficient funds to honor the transaction. If both tests are passed, the database is updated with new account balances. In the case when the

value of the output exceeds the preliminary input, the difference constitutes a *transaction fee* (Kroll *et al.*, 2013), which is paid to the participant who successfully appends the transaction to the blockchain. The transaction can be treated as finalized when it achieves multiple confirmations. There is no fixed number for that, but six is a commonly accepted heuristic (Narayanan *et al.*, 2016).

For a majority of cryptocurrencies, all participants are given equal rights. Everyone can join the network by downloading a *wallet* software, which generates addresses and private keys. The user starts connecting with other nodes by sending her *seed node* message to the address she knows. The message asks the recipient to share all the other addresses in the network that this node knows about.

The aim is to build the network in order to publish, confirm and complete the transactions. When the user sends a transaction, her node distributes the message to all the nodes it is peered with. Each recipient individually checks and determines if it accepts the transaction. The process includes transaction validation with the current blockchain, checking if the outputs have not been already spent, rejecting already seen transactions, and checking the validity of the script.³ If approved, the message is further distributed in the same way.

This process is called a *flooding* algorithm. Each node that receives the message puts it in the pool of transactions not attached to the blockchain. The transactions in the pool are not further broadcast by the nodes in order to prevent the creation of the indefinite loop. It is estimated that there are approximately 10,000 permanently connected nodes which fully validate every transaction and (as of Q1 2019) 35 million Blockchain wallet users (Statista, 2019). Such an outcome is possible because the majority of them are *lightweight* wallets (Narayanan *et al.*, 2016).

Fully validating nodes must be permanently connected to the Internet to receive new transactions and they must also store the entire blockchain and unspent transactions pool, which is out of reach for the average desktop computer. The lightweight nodes, on the other hand, do not store the entire blockchain, but only pieces which are necessary for validation of

³There is no obligation for the node to comply with all checks. A majority comply with the rules in order to protect the smooth operation of the network. Some may deter from this strategy and try to forward double spends, or similarly invalid transactions. The attempt ultimately fails, because only one transaction can be added to the block, and when it happens, the other nodes will drop the invalid transaction from their memory pool.

the transaction that concerns them. They rely on the *miners*, the owners of fully validating nodes who append transactions into the blockchain. They made a significant investment in the mining process and therefore must be certain that the transactions they are processing are valid.

The wallet is a comprehensive tool helping the user to manage their account. Besides generating keys, the software also creates transactions that are sent to the network, collects incoming and outgoing transactions to show the balance of available funds, and securely stores the user's private keys. If a private key is lost, there is no possibility to sign any transaction or access the funds in the ledger. Coins are not stored in the wallet or in the device where the software is installed but recorded in the ledger, which holds the balance of funds for each address.

Franco (2014) distinguishes two major groups of wallets: offline and web wallets. They differ by their connection to the Internet and the fact that the offline wallets are predominantly managed by the user itself, while in the case of web wallets, funds are transferred to the third party which manages them on behalf of the user. Both of these leaves web wallets at greater risk of being compromised. Web wallets are a subgroup of the larger category called online or *hot wallets*, which are any device holding a wallet and being connected to the Internet at the same time.

Offline wallets sign transactions offline. Before it takes place, the private key should be imported from a cold storage (USB, a piece of paper known as a *paper wallet*⁴ or any other storage medium which cannot be accessed from the Internet). We can find a physical cryptocurrency in the form of a coin or paper, with the private key hidden behind a tamper-proof mechanism. Among offline wallets, there are also independent *hardware wallets*; the devices both store private keys and receive, sign, and return the transaction.

Web-based wallets are online accounts provided by a third party where users deposit their funds (Franco, 2014). The transaction cost will be lower if the operator decides to pool many transactions before sending them into the blockchain, and the outsourcing of account management makes Web wallets more accessible to the first-time users.

Approximately three-quarters of the providers do not store private keys (Hileman and Rauchs, 2017), which means that they do not have a control over users' funds. These are named *hybrid web wallets*. For the

⁴Although it is an accepted name, a paper wallet is not technically a wallet, because it is not able to perform all the other tasks that the software named *wallet* does.

remaining minority, there is a risk if a provider is fraudulent and aims to steal the clients' funds. Web wallets are also exposed to hacking attacks. For this reason, their use is predominantly limited to day-to-day financial operations, which matches the fact that the mobile format is the most popular one among wallet providers.

Among the alternatives, we find the *brain wallets* (Franco, 2014) that has a long password which is supposed to be remembered by a user. We also distinguish *deterministic wallets*, which generate many addresses and their associated private keys from a common private key. Finally, there are also *multi-signature wallets* which increase security by requiring several signatures to unlock funds and *vault wallets* that provide custody solutions for enhanced security management.

As described above, users can make the transactions in cryptocurrency using wallets. However, because of the fact that the cryptocurrencies are currently not a widely accepted payment method, we can expect that for the majority of users, the aim is to exchange them into the national currencies. In order to do that, the agent must approach the currency exchanges. They are the first sector that emerged in the cryptocurrency industry, have the highest number of operating entities and employees (Hileman and Rauchs, 2017) and remain the biggest driver of industry growth (Rauchs *et al.*, 2018). The first one appeared in 2010, and today, there are over 500 exchanges in operation.

The exchanges function similar to the traditional bourses by matching the demand and supply orders. Such transactions are not updated in the blockchain. The exchange registrar updates its contracts with the users involved in the exchange, and no money movement actually takes place. Alternatively, a person can access selected cryptocurrencies using ATMs, at private meetings or trading events. They can exchange real cash for the physical cryptocurrency or use *payment providers*.

The role of payment providers can be placed in between wallets and exchanges. Their primary function is being a payment link between the cryptographic and real worlds. They are used by the merchants who accept cryptocurrency payments (Narayanan *et al.*, 2016), for business-to-business transactions and individual money transfers such as bill payments (Hileman and Rauchs, 2017).

In summary, the key crypto-asset industry segments are Storage, Payments, Exchange and Mining (Rauchs *et al.*, 2018). Over the years, the provision of multiple crypto-assets expanded and, as of the end of 2018, Bitcoin (92%), Ether (79%), Litecoin (61%), Bitcoin Cash (47%)

and Ripple (41%) were supported by the largest share of providers (excluding miners).

2.2 Blockchain

The blockchain derives its name from a chain of *blocks*, in which the data (ordered transactions) are grouped. Once the information is added to the blockchain, it cannot be altered, and its security relies on the verification mechanism used. The cryptographic links between the blocks create the record of all past transactions. It is a peer-to-peer network, where a node is any computer system with the software installed in it.

Each block stores the data of the transactions (Nian and Chuen, 2015) whose size is determined by the number of inputs and outputs. Every block is built from a body, where transactions are stored, and a header. The header includes identifiers, such as the hash value of the previous block of the chain, the hash of all the transaction hashes in the block, and the bit field of the current target value. When the block is validated, a computer must solve a mathematical puzzle of finding the hash of a block's header lower than or equal to the current target.

All blocks combined together result in a complete history of all transactions ever made, which can be viewed by accessing the cryptocurrency software. They are grouped by order, where the most recent blocks are chained to the former ones, up to the genesis block. The *Hashcash* function transforms the input message into the bit digest. The computer must solve the aforementioned mathematical problem in order to add the next block into the blockchain, and the solution can be found only by random guessing. The first one which succeeds broadcasts it to the network and it is accepted as the next block in the chain.

The validation process is called *mining*. The goal of the system is to add a block to the chain in a timeframe specified in the code (Dwyer, 2016). Therefore, the difficulty of finding a solution is dynamically adjusted. If two miners find the solutions at the same time and broadcast them to the system, it is the longest block (the one which all miners will switch to and start adding the additional blocks) which is preserved. The other one is abandoned and becomes an *orphan block* (Franco, 2014). The agreement on the longest blockchain is named a *consensus* (Dwyer, 2016). Other miners express their approval of the block by including its hash in the next block they create (Narayanan *et al.*, 2016). In order to be accepted, all the transactions in the block must be signed by valid signatures.

Bitcoin is a proof-of-work system, which means that the selection of a random node is approximated by choosing nodes in proportion to a resource, i.e., computing power (Dwyer, 2016). Because of concerns regarding the efficiency of the system, alternative mechanisms for reaching consensus have been developed, such as the proof-of-stake or proof-of-importance.

Blockchain as a data structure has found multiple applications beyond the cryptocurrencies market (Swan, 2015). The new cryptocurrencies proposed additional solutions, such as smart contracts software *that codifies legal procedures with decentralized autonomous execution* (Williams, 2016). Its possible applications include the property market, (Dwyer, 2016), finance industry, voting mechanisms, supply chain and IoT projects (Pilkington, 2015). Visa, Nasdaq, IBM, Microsoft and other institutions invested in the development of this technology (Frost & Sullivan, 2016).

There is a small group of cryptocurrencies which does not have a blockchain. The most widely used one is Ripple, which operates with a *global consensus ledger* as an alternative (Hileman and Rauchs, 2017). It requires no mining, but instead verifies transactions with an algorithmic consensus. Therefore, as opposed to Bitcoin, the verification is instantaneous. On the other hand, it uses a centralized ledger instead of a decentralized blockchain.

2.3 Mining

In the absence of a central authority, the community is responsible for adding the data to the blockchain. Miners carry out this task. The source of income for them is the *block reward*, i.e., the newly generated coins and/or transaction fees (if any).

The miner receives a block reward only if it is appended into the blockchain. This mechanism incentivizes the nodes to behave in the way that is accepted by the majority of the miners and penalizes those that are trying to act dishonestly. As a result, the creators of the invalid blocks never get paid. On the other hand, the transaction fee is purely voluntary and variable. It is determined by the creator of the transaction who may choose to make the total value of the outputs less than the value of the inputs. The miner who first puts such a transaction to the blockchain collects the difference. When block rewards disappear completely, we may speculate that fees will become mandatory in order to ensure the smooth processing of the transactions.

By looking into proof-of-work mechanism, Kroll *et al.* (2013) estimate that the equilibrium situation would imply small, but non-zero, transaction fees. The miners can benefit from cooperation. However, because each miner has an incentive to include every transaction whatever be the fee, any other outcome is not stable. As a result, they are trapped in the classic prisoner's dilemma. The miners ensure currency survival by confirming the validity of transactions, and their dedicated computer power is the guarantee of system security. When the system starts to rely solely on the transaction fees, Houy (2014) suggests that the only way to correct this market inefficiency is by integrating into the protocol the block size constraint or a built-in transaction fee.

Similar to any other user, the miner joins the network and connects with other nodes (Narayanan *et al.*, 2016). She subsequently starts to listen to the transactions on the network and validates them. At the same time, the miner needs to maintain the blockchain and wait for the new blocks. She must first ask other nodes to provide her with the historical blocks already included in the chain. Next, the miner starts validating each block she receives by examining each transaction it contains and checking if the block has a valid *nonce*. As soon as the miner has the updated blockchain, she can start the ultimate task of building her own block. In order to do that, she groups the transactions from the waiting pool, confirms that each of them is valid, and clusters them into the new block. When completed, the miner must find a nonce which makes the block valid, meaning that she must solve the hash function matching current prerequisites. If she manages to do it before the other users, she messages the block to other nodes. Only if other miners accept the block and start mining on top of it, the miner receives the reward. It may happen that two miners distribute the block at the same time. In such a case, even if the block contains all valid transactions, only one block becomes appended to the blockchain and the other one remains orphaned.

We now look at how the miners' community is structured. *Solo mining* lets the owner of the device compute solutions to the hashing function individually. If successful, one is paid the entire reward. The probability of success is low and variability high. Bhaskar *et al.* (2015) estimate that a well-equipped miner earns a reward on average every three months. Because of the random nature of the process, the lags can take too long a time to make an investment profitable. Alternatively, players can get involved in *mining contracts* or *mining pools*. Mining contracts offer the possibility of investment in the mining process without managing

hardware or software. Contracts provide mining services or mining shares in the large-scale mining centers. This includes cloud mining, i.e., using shared processing power run from remote data centers.

The mining pools are the groups of miners who contribute their resources into joint mining which generates higher hashing power. The probability of mining the block increases with the amount of resources dedicated to the process, but the reward is split between participants based on their individual contributions. Such organized groups of miners have also a higher influence on protocol content. In 2017, five mining pools controlled 79% of the market, with three-quarters of all mining pools being based in China and the USA.

2.4 *Vulnerability to Cyber Attacks*

The attacks on the system can be grouped into two categories. The first includes the attacks on a single user attempted by trying to find out the person's private key or misleading her into sending funds to the wrong address. These are performed either virtually by *address tampering* (Franco, 2014) (largely impossible as most of the cryptocurrency codes have protections against it), or physically by substituting a physical QR code sticker with the illicit one in the places that accept Bitcoin payments.

The second category includes the attacks made on the blockchain itself. We do not describe all the possible attacks that may occur, nor we provide all their consequences. Our aim is to outline some possible vulnerabilities.

The most discussed one is called a *51% attack* (Franco, 2014). The attack is performed when a person commands a hash rate equal to or larger than the hash rate of the rest of the network. Such an individual may then try to perform a *double-spent attempt* or prevent other miners from mining the blocks, and ultimately destabilize the system.

If one would wish to change the blockchain at a certain point, she would have to mine again all the blocks from that point in time to the present. Additionally, she would need to surpass the pace of the current new block creation. In order to make it possible, the attacker would need to command a hash rate equal to the rate of the rest of the network. The probability of success decreases exponentially with the control rate smaller than 50% and the number of blocks required to outpace.

In the case of *race attack*, the attacker could double-spend by sending *a transaction to the nodes close to the vendor and a different transaction*

to many other nodes in the network (Franco, 2014, p. 115). If the vendor accepts payment on an unconfirmed transaction by checking only a few nodes, the attack is successful.

A *Finney attack* was discovered in 2014 by Hal Finney. It happens when a miner secretly mines a block, including in it a transaction between two of her addresses, which has never been broadcast to the network. Before releasing the block, the attacker sends a double spend included in her transaction. If the victim accepts the payment, the miner releases a secret block. In contrast to the 51% attack, the action does not require a high hash rate. In order to defend themselves against such a situation, the users should require at least two conformations for their transactions.

Lastly, we face attacks on the infrastructures where blockchain is hosted or the surrounding institutions such as cryptocurrency exchanges. During the attack on the Ethereum blockchain, hackers sent the spam that used up *gas*, the network's computational power, in order to slow down activity in the network (Hertig, 2017a). In another instance, 3.8 million worth of Ether has been drained from the DAO, the autonomous organization supporting the operations of the Ethereum network, which led to a fork and the currency split.

3. The Governance of Cryptocurrencies

In the previous section, we used Bitcoin as a case study to show the technological innovations behind cryptocurrencies and how they can be employed by regular users. Still, there is a consensus in the academic literature on the fact that what makes cryptocurrencies unique is not only the technology that powers them, but the way in which the technology is used to govern over the currency — the fact that the blockchain is distributed among a network of peer-to-peer users in a non-hierarchical fashion (Hsieh *et al.*, 2017; Evans, 2014; Swanson, 2015).

Apart from being a distinctive feature of cryptocurrencies, their governance is also considered to be a significant factor that affects their performance. For this reason, in this section, we synthesize the views present in the academic literature on the different approaches that can be taken in governing a cryptocurrency. We divide the section into two parts. Since the blockchain is a defining feature for most cryptocurrencies, the first part focuses on governance within the blockchain. The second part analyzes the governance of institutions that manage the blockchain.

3.1 *Governance within the Blockchain*

One of the innovative aspects behind cryptocurrencies is that they were the first organizations to use the blockchain technology. As explained in the first section, digital currencies that used cryptography to secure their operations and assure anonymity existed before Bitcoin, but it was Nakamoto (2008) who first put into practice the idea of a ledger that can be operated without a central authority. Since users do not require a third party to centralize the management of the system, blockchain-based organizations are usually assumed to manage transactions without the need for an intermediary. This description is misleading, however, because the blockchain in itself is the intermediary and its operability and economic efficiency depend on its ability to attract the workforce to work for it (Evans, 2014), which means that the design of the blockchain itself bears an important role in the success of a cryptocurrency.

Moreover, the novelty of a blockchain-based organization does not reside in its capacity to remove people from the operation of the blockchain, but rather in its ability to put software at the core of the organization, leaving human actors on the margins (Hsieh *et al.*, 2017). It is these actors that we are concerned with in this section. More specifically, we first look at actors that can bring modifications to the blockchain, *given a certain blockchain protocol*, and then we survey different approaches to structure a blockchain and how they impact the authority and incentives of these actors.

In the literature, the actors mentioned above are usually labeled as *miners*. This term comes from the fact that cryptocurrencies use cryptography by asking agents that operate in the blockchain to solve costly tasks. These tasks — meant to verify and record transactions into the blockchain — are probabilistically impossible to deconstruct, thus preventing malevolent agents from tampering with the system, and also require significant technological resources from the miners.

Hsieh *et al.* (2017, p. 8) describe miners as having two roles: Firstly, they act as “employees” by following the rules imposed through a software-embedded protocol in order to accomplish certain tasks. The protocol sets the timing and priority of transactions, which Yermack (2017, p. 26) compares to the rules of a regular stock exchange. Secondly, they act as *decision makers*, as they can decide which transactions to accept in the blockchain or not. By doing this, they have the agency to say which is the correct version of the blockchain. It is this second role that can affect

the stability of cryptocurrencies, if small groups of users can exert outsized power over the network (Kroll *et al.*, 2013).

3.1.1 *The centralization of the blockchain*

Having defined the actors that are relevant for governing within the blockchain, we now look at the relations between them. When analyzing the networks formed by miners, the academic literature usually focuses on one feature of these networks — their level of decentralization. For a few years after Bitcoin was invented, the academic literature ignored the governance of cryptocurrencies (Yermack, 2017), and this gave birth to a dichotomous view of currencies, where at one end there was the fully decentralized Bitcoin, and at the other end the centralized models on which traditional currencies operated. In fact, blockchain-based organizations rather lie on a spectrum of decentralization, which can be divided into three broad categories: centralized, decentralized and distributed networks.

Centralized networks have a central node and a set of peripheral nodes which are only connected to the central node through which all communication is conducted. From a governance perspective, there is nothing innovative in these networks and indeed most cryptocurrencies do not want to replicate this model. Still, the technology employed by blockchains can be of interest for the redesign of centralized networks, and there have been suggestions that central banks could create their own centralized cryptocurrencies (Piscini, 2015; Broadbent, 2016).

Distributed networks lie at the other end of the spectrum and consist of a set of nodes that are all connected to each other. This is an idealistic design of a network, where all nodes have equal authority and there is no need for intermediaries when a transaction is added to the ledger, as the ledger is distributed among users who compete to add information to it (Weber, 2016). The currency that resembles the most this kind of network is Bitcoin. Bitcoin was envisioned by Nakamoto as an egalitarian network and it was assumed to be self-governing. Still, Bitcoin moved away from this network structure over time for reasons that we explore below.

Decentralized networks exist somewhere in between the distributed and the centralized models. These networks do not have a central node that has full authority over the blockchain, but there are some nodes in the network

that can act as intermediaries for transactions. Moreover, these networks differentiate themselves from distributed networks by the fact that nodes do not have equal authority in the blockchain. Most of the cryptocurrencies today operate on a model like this.

Lo and Wang (2014) suggest three reasons why Bitcoin moved away from the fully decentralized network model. The first reason is the apparition of intermediaries outside of the blockchain protocol. These intermediaries facilitate certain types of financial transactions with cryptocurrencies (such as exchanging cryptocurrencies with legal tender) and can gain a lot of influence over the cryptocurrency ecosystem (such was the case of the Mt. Gox exchange). The second reason is the apparition of intermediaries whose purpose is to connect end-users to the network in an easier manner, such as electronic wallets.

The third reason why cryptocurrencies that employ proof-of-work (like Bitcoin) become more centralized is the collusion of groups of miners into mining pools that do the “mining” operations in a centralized fashion. Out of the three reasons, this is the most important one for the stability of the system and also the one that is related to the operability of the blockchain protocol. Mining pools arise for two reasons. The first reason is that the rewards from mining are highly volatile. Miners gain a return from the process of mining when they solve the cryptographic puzzle embedded in the verification mechanism.

Since the puzzle is a complex computational task, with its difficulty increasing over time, the probability of solving the puzzle is small, which makes the rewards from mining uncertain. If we assume that a mining pool can harness the same technology as a solo miner, joining a mining pool does not increase the expected value of the return from mining, but reduces the variance of the reward, since all the computing power in a pool is used aggregately and rewards are shared among users (Eyal, 2015).

But mining pools can also harness better technology, and this is the second reason why miners are incentivized to join mining pools — this is especially relevant as rewards from mining become smaller as the currency approaches its cap, thus making mining become exponentially harder over time (Eyal, 2015). This increase in difficulty can be offset only by acquiring more complex equipment to mine. As Tindell (2013) points out, whilst in the early stages of Bitcoin a regular PC was powerful enough to make mining a profitable endeavor, in 2013 specialized equipment was already necessary. Nakamoto did not foresee this development, as the stability of the blockchain was based on the idea that all nodes in the network are equally powerful (hence, the idea of *one-CPU-one-vote*).

Currently, mining technology becomes increasingly more expensive, in what certain authors have qualified as an arms race (Tarasiewicz and Newman, 2015). Mining pools turn into large-scale businesses that exhibit economies of scale and require specific conditions in order to operate efficiently, which impose significant barriers to entry for newcomers — an article from *The Economist* describes how, currently, mining pools are relocating to areas that have low temperatures and can provide cheap energy in order to cut costs (The Economist, 2017).

3.1.2 Verification mechanisms

The literature has also focused on another aspect of cryptocurrencies that is significant in determining the governance of blockchains: the verification mechanism. The verification mechanism lies at the core of the blockchain and it is instrumental in establishing the level of centralization in the network and the authority relationships between miners.

Verification mechanisms represent the technology that enables cryptocurrencies to have an innovative governance structure. There are significant differences between various mechanisms, but what all of them have in common is that they ask miners to dedicate significant resources to add valid transactions to the blockchain. The vast amount of resources spent creates a structure that is hard to tamper with and thus it makes it highly improbable for a user to fraud the system. Verification mechanisms can be classified based on two criteria: the nature of the task miners are asked to solve, and the distribution of power among miners. Verification mechanisms can prioritize the decision of some miners and thus determine the level of centralization within the blockchain.

The most common verification mechanism is called proof-of-work and it is the one employed by Bitcoin and by almost all of the alternative currencies that copied the source code of Bitcoin (Bonneau *et al.*, 2015). Proof-of-work is a system with significant disadvantages and there are multiple verification mechanisms that have been created in the recent years in order to address the deficiencies. We dedicate the rest of this section to an overview of some of the most common verification mechanisms.

Proof-of-work

Proof-of-work was first used in a cryptocurrency by Nakamoto (2008) and it is based on Adam Back's Hashcash algorithm (Back, 2002). The distinctive feature of this algorithm is that it allows users to add

elements to the blockchain based *solely* on their ability to solve a computationally intensive puzzle. Proof-of-work users do not have to own currency in order to mine it. Mining power is proportional to the computing power that each user has, which means that currencies that use proof-of-work are usually associated with a high degree of decentralization (Hsieh *et al.*, 2017). If there are no significant differences in the computing power of agents, this mechanism does not only facilitate the validation of individual transactions, but also creates a credible commitment against attacks on the blockchain, since it becomes increasingly more difficult for a malevolent actor to tamper with the structure of the ledger, as the effort required for an attack increases proportionally with the number of blocks that the user wants removed (Catalini and Gans, 2016).

Lee (2016) points out that proof-of-work is considered to have three disadvantages: The first disadvantage is the high amount of computational power that is required. Computational power is an issue, in particular for proof-of-work algorithms because they are egalitarian in nature, meaning that all users have roughly the same incentive to compete (adjusted to their available CPU), but only one of the users actually solves the puzzle, which means that large amounts of computational effort and electricity are wasted (Papadopoulos, 2015, p. 159). This problem is aggravated by the fact that the difficulty level of the puzzles increases over time.

The second disadvantage comes from the fact that in a proof-of-work system, miners are incentivized to bear the costs of mining by being rewarded with new coins and transaction fees, but the rate of new coin creation is usually set to decrease over time. This can disincentivize miners from investing resources into mining, which is detrimental for regular users of Bitcoin (Davarpanah *et al.*, 2015).

Finally, the decentralized nature of proof-of-work algorithms does not prevent attacks that can modify the components of the blockchain. Attacks can still be conducted by an agent that amasses more than half of the computing power of the whole network. The risks of such “51% attacks” has increased with the apparition of mining pools, and some authors argue that the centralization of the mining process is inevitable for these cryptocurrencies, as the increasing costs and volatility of returns incentivize users to cooperate (Davarpanah *et al.*, 2015).

Proof-of-stake

The main difference between proof-of-work and proof-of-stake mechanisms lies in the way voting power is distributed among users.

In proof-of-work, the voting power is proportional to the computational power of each user. In proof-of-stake, the voting power depends on some posted collateral that each user has, which usually is the number of the coins they own (Mazieres, 2015). Since computational power is not required, this means that the operating costs are smaller, which also reduces the necessary values of transaction fees (Davarpanah *et al.*, 2015). The reward is also not fixed, as in the case of proof-of-work, and miners receive a rate of return akin to a regular interest rate (Davarpanah *et al.*, 2015, p.13). Moreover, because each miner has a vote proportional to their stake, 51% attacks are not expected from a rational user as this would also involve losing their stake in the currency. Still, a disadvantage of proof-of-stake mechanisms is that they create more centralized networks compared to proof-of-work, as users that own more resources also have more power (Lee, 2016). Examples of cryptocurrencies that use proof-of-stake are Nxt and NeuCoin (Davarpanah *et al.*, 2015). Ether, the currency associated with the Ethereum project, is functioning on a proof-of-work mechanism, but it is planning on transitioning to proof-of-stake (Hertig, 2017b).

Another addition to a verification mechanism that needs to be mentioned here, although it is also compatible with proof-of-work-based currencies, is the introduction of a checkpointing mechanism, which aims to prevent 51% attacks. Checkpoints are hard-coded blocks that cannot be rewritten. This means that even if a group of users gains the necessary power to attack a blockchain, their attack would not be able to go past certain blocks in the ledger (Tarasiewicz and Newman, 2015). Feathercoin and Peercoin are examples of currencies that adopted this mechanism (Davarpanah *et al.*, 2015). Even if this measure clearly secures a cryptocurrency, it is criticized for the fact that it is a form of centralization and it implies putting trust in a user that creates the checkpoints.

Alternatives to proof-of-stake

All proofing mechanisms involve imposing a cost on mining (forwarded by a reward) in order to secure a cryptocurrency. What proof-of-stake does is that it replaces the operational cost required in proof-of-stake with a capital cost — the financial stake that one has in a currency.

Many new cryptocurrencies try to harness the benefits of both proof-of-work and proof-of-stake by employing mixed verification mechanisms. Peercoin is such a currency, which employs proof-of-stake in order to offset the negative impact of mining diminishing returns generated by

proof-of-work. The system accomplishes this by creating a steady inflation rate of 1% through proof-of-stake mining.

Since the apparition of proof-of-stake, multiple new algorithms have emerged. Among these algorithms, we can mention the following: proof-of-burn (P4Titan, 2014) (which asks miners to destroy some coins at each verification), proof-of-luck (Milutinovic *et al.*, 2016) (which introduces a lottery in the mining process) or proof-of-time (Intel, 2015) (which uses a lottery and enforces a time frame on the mining process).

3.2 *Governance of the Blockchain*

Up until now, we described various ways in which the protocol of the blockchain can be organized. In this section, we look at the institutions that take decisions about the way the protocol is organized. Since the creation of Bitcoin, hundreds of cryptocurrencies have been launched, which came with numerous governance structures of these alternative currencies. There is no comprehensive overview of all these structures in the literature, and this section will not attempt to fill this gap. Instead, we first describe the governance structure that is embraced by most projects and that is also the focus of most academic research studies — the open-source-like organization — and then briefly present the alternative organizational structures that some of these currencies embrace.

One of the goals of cryptocurrencies is to create a currency that can function without its users having to trust a central authority. This ideal is reflected not only in the employment of blockchain, but also in the way the blockchain protocol is managed. Most early cryptocurrencies have a simple governance structure, with a group of core developers, usually overseen by a chief scientist, that implement all the necessary changes in the blockchain protocol. Changes to the source code can be proposed by anyone. The decision on what changes are to be made can be taken either by the group of core developers or through a democratic procedure where miners vote on proposed changes. Hsieh *et al.* (2017) classify these decision-making procedures by using a scale of decentralization, where at one end, core developers concentrate all power and implement changes with no external input, and at the other end, there is a formal voting mechanism. Bitcoin, for instance, lies somewhere in the middle of this scale, with non-controversial issues being decided by a group of core developers, whereas controversial issues are decided through informal

voting procedures on online forums (Papadopoulos, 2015, p. 159). The open-source nature of the code and the fact that cryptocurrencies function because of a group of volunteer developers together with a decentralized group of supporters (the miners) made some authors compare cryptocurrencies with open-source projects (Kroll *et al.*, 2013).

Still, there are authors that point out that there are significant discrepancies between an open-source project and a cryptocurrency, discrepancies that can threaten the stability of these organizations. Evans points out how one of the significant differences is the divergence in interests between miners and developers. Whereas in an open source project like Wikipedia, the goals of the core developers are the same as the goals of the regular contributors (to create a repository of free articles), in a cryptocurrency miners have goals different from those of the developers. This happens because in an open-source project, contributors work for a non-pecuniary interest that also defines the existence of the project, but in the case of cryptocurrencies, miners work in order to obtain revenue (Evans, 2014).

Miners require an incentive scheme to work, and the existence of a group of core developers that can take decisions regarding it without their consultation can significantly destabilize a currency. Indeed, multiple currencies, such as Litecoin (Rizzo, 2017) or Ethereum, have been affected by such disagreements between groups of miners and the core developers, either because core developers took decisions without consulting miners or because of the lax voting procedures that do not incentivize stakeholders to reach a consensus. As a consequence, some authors have suggested that cryptocurrencies need stronger governance structures (Kroll *et al.*, 2013), while others have described the current institutional arrangements of most cryptocurrencies as going against the democratic ideals they propose.

Still, there are an increasing number of cryptocurrency projects that embrace more conventional governance frameworks. This is made possible, to an extent, by the existence of verification mechanisms that allow for more centralization, and it is motivated by the fact that some of these projects want to create stronger links with the financial sector instead of creating a system parallel to it. Such an example is Ripple, a cryptocurrency and blockchain-based payment protocol that embraces a regular corporate structure, which Evans (2014, p. 16) compares to Google's governance structure over Android.

The current state of cryptocurrencies does not offer a clear model of the way they should be governed, although there is an emerging consensus in the academic literature that organizations that retain the decentralized nature of the blockchain, which differentiates them from other financial institutions, while embracing a more complex and centralized governance structure, tend to perform better. This view is supported by the findings of Hsieh *et al.* (2017, p. 3) who analyzed the correlation between the return of investment in various cryptocurrencies and their governance structure, and observed that returns increase as the blockchain is more decentralized, but the decentralization of the organization negatively affects returns.

4. Conclusion

This chapter aims to familiarize the reader with the concept of cryptocurrencies and their current market structure. Based on the academic literature and on market news, we provide an overview of the basic features characterizing these alternative payments systems. In four sections, we introduce the economic origins of cryptocurrencies, provide an introduction to their technical architecture and supporting systems, explain their different forms of organizational structures, and finally provide examples of different cryptocurrency projects. We hope that this work is a useful contribution in synthesizing the present knowledge of the diversified world of cryptocurrencies and in providing an introduction to the subject for future research.

Acknowledgments

Financial support by the University of Manchester's FinTech Initiative is gratefully acknowledged.

References

- Abrams, R., and N. Popper. 2014. "Trading Site Failure Stirs Ire and Hope for Bitcoin." *The New York Times*, 25th February. p. B1(L). *Gale Academic OneFile*, <https://link.gale.com/apps/doc/A359788335/AONE?u=jrycal5&sid=AONE&xid=0cfb5c53>.
- Ametrano, F. M. 2016. "Hayek Money: The Cryptocurrency Price Stability Solution." Available at SSRN: <https://ssrn.com/abstract=2425270>.

- Back, A. 2002. "Hashcash — A denial of service counter-measure." www.hashcash.org/papers/hashcash.pdf.
- Bhaskar, N. D., L. P. Nian, and D. L. K. Chuen. 2015. "Bitcoin IPO, ETF, and Crowdfunding." In D. L. K. Chuen (ed.), *Handbook of Digital Currency*, Chapter 27, 529–557, Amsterdam: Elsevier.
- Bonneau, J., A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. 2015. "Research perspectives and challenges for bitcoin and cryptocurrencies." MIT Computer Science and Artificial Intelligence Laboratory.
- Broadbent, B. 2016. "Central banks and digital currencies." *Speech at London School of Economics*, Bank of England.
- Catalini, C., and J. S. Gans. 2016. "Some simple economics of the blockchain." *National Bureau of Economic Research (NBER) Working Paper No. 22952*.
- Chaum, D. 1983. "Blind Signatures for Untraceable Payments." In D. Chaum, R. L. Rivest, and A. T. Sherman (eds.), *Advances in Cryptology: Proceedings of Crypto 82*, 199–203. Amsterdam: Elsevier.
- . 1982. "Computer systems established, maintained and trusted by mutually suspicious groups, PhD dissertation." *Electronics Research Laboratory*, University of California.
- Christin, N. 2012. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace." CyLab, Carnegie Mellon University.
- Coppola, F. 2016. "Ethereum's Latest Hard Fork Shows it has a Very Long Way to Go," *Forbes*, 16th November.
- Davarpanah, K., D. Kaufman, and O. Pubellier. 2015. "NeuCoin: The First Secure, Cost-Efficient and Decentralized Cryptocurrency." Available at <https://arxiv.org/abs/1503.07768>.
- De Filippi, P., and B. Loveluck. 2016. "The invisible politics of bitcoin: Governance crisis of a decentralized infrastructure." *Internet Policy Review* 5(3). <https://doi.org/10.14763/2016.3.427>.
- Dwork, C. 2006. "Pricing Via Processing or Combating Junk Mail," In: *Advances in Cryptology — CRYPTO 2006: 26th Annual International Cryptology Conference*, 139–147.
- Dwyer, G. P. 2016. "Blockchain: A Primer." Available at SSRN: <https://ssrn.com/abstract=2900450>.
- Evans, D. S. 2014. "Economic aspects of bitcoin and other decentralized public-ledger currency platforms." *Coase-Sandor Institute for Law & Economics Working Paper No. 685*.
- Eyal, I. 2015. "The Miner's Dilemma," paper presented at the 2015 *IEEE Symposium on Security and Privacy*. <https://ieeexplore.ieee.org/document/7163020>.
- Franco, P. 2014. *Understanding Bitcoin: Cryptography, Engineering and Economics*. Hoboken, NJ: Wiley.

- Frost & Sullivan. 2016. "The Definitive Blockchain Conference — Consensus." Available at <http://www.frost.com/sublib/display-report.do?id=9B06-00-15-00-00>.
- Golumbia, D. 2016. *Politics of Bitcoin: Software as Right-Wing Extremism*. Minneapolis, MN: University of Minnesota Press.
- Haber, S., and W. Scott Stornetta. 1991. "How to Time-Stamp a Digital Document." In A. J. Menezes and S. A. Vanstone (eds.), *Advances in Cryptology-Crypto '90: Proceedings*, 437–455. Springer. Berlin.
- Hertig, A. 2017a. "Ethereum Developers Stymie Blockchain Spammer's New Attack, CoinDesk, 1st June." Available at <https://www.coindesk.com/ethereum-developers-stymie-blockchain-spammers-latest-attack/>.
- . 2017b. "Ethereum's Big Switch: The New Roadmap to Proof-of-Stake." Coindesk, 5th May, Available at <https://www.coindesk.com/ethereums-big-switch-the-new-roadmap-to-proof-of-stake/>.
- Hileman, G. 2014. "From bitcoin to the brixton pound: History and prospects for alternative currencies." paper presented at the *International Conference on Financial Cryptography and Data Security 2014*.
- Hileman, G., and M. Rauchs. 2017. "Global Cryptocurrency Benchmarking Study." Working Paper, Cambridge Centre for Alternative Finance.
- Houy, N. 2014. "The economics of bitcoin transaction fees." *Working Paper GATE 2014–07*.
- Hsieh, Y.-Y., J.-P. Vergne, and S. Wang. 2017. "The Internal and External Governance of Blockchain-Based Organizations: Evidence from Cryptocurrencies." Available at SSRN: <https://ssrn.com/abstract=2966973>.
- Huckle, S., and M. White 2016. "Socialism and the Blockchain." *Future Internet* 8:4, 49.
- Intel. "Introduction to Sawtooth." 2015. <https://intelledger.github.io/introduction.html>.
- Kaminska, I., and P. Murphy. 2017. "Crypto currency offerings spur speculation frenzy." *Financial Times* 14th May.
- Kroll, J. A., I. C. Davey, and E. W. Felten. 2013. "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries," paper presented at the Proceedings of WEIS.
- Lee, L. 2016. "New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market," *Hastings Business Law Journal* 12:2, 81–132.
- Lo, S., and J. C. Wang. 2014. "Bitcoin as Money?" *Current Policy Perspectives*: Federal Reserve Bank of Boston.
- Lustig, C., and B. Nardi. 2015. "Algorithmic Authority: The Case of Bitcoin." In: *HICSS 2015, 48th Hawaii International Conference on System Sciences*, 743–752.
- Mazieres, D. 2015. "The stellar consensus protocol: A federated model for internet-level consensus." *Stellar Development Foundation*. <http://www.scs.stanford.edu/17au-cs244b/notes/scp.pdf>.

- Milutinovic, M., W. He, H. Wu, and M. Kanwal. 2016. "Proof of luck: An efficient blockchain consensus protocol." paper presented at the Proceedings of the 1st Workshop on System Software for Trusted Execution.
- Nakamoto, S. 2009. "Bitcoin Open Source Implementation of P2p Currency." Available at <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>.
- . 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System."
- Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. 2016. *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton, NJ: Princeton University Press.
- Nian, L. P., and D. L. K. Chuen. 2015. "Introduction to Bitcoin." In D. L. K. Chuen (ed.), *Handbook of Digital Currency*, Chapter 1, 5–30, Elsevier.
- P4Titan 2014. "Slimcoin a Peer-to-Peer Crypto-Currency with Proof-of-Burn." Available at www.slimcoin.club/whitepaper.pdf.
- Papadopoulos, G. 2015. "Blockchain and Digital Payments: An Institutional Analysis of Cryptocurrencies." In D. L. K. Chuen (ed.), *Handbook of Digital Currency*, Chapter 7, 153–172, Amsterdam: Elsevier.
- Pilkingtong, M. 2015. "Blockchain Technology: Principles and Applications." In F. X. Olleros and M. Zhegu (eds.), *Research Handbook on Digital Transformations*, Cheltenham: Elgar.
- Piscini, E. 2015. "State-Sponsored Cryptocurrency, Deloitte." Available at <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/strategy/us-cons-state-sponsored-cryptocurrency.pdf>. Accessed 31st August 2017.
- Popper, N. 2016. "A bitcoin believer's crisis of faith." The New York Times, 17th January, p. 1(L). Gale Academic OneFile, <https://link.gale.com/apps/doc/A440094953/AONE?u=jrycal5&sid=AONE&xid=dce66479>.
- Popper, N. 2017. "Bitcoin Technology to Power Database Used by World's Largest Banks." The New York Times, 10th January, p. B4(L). Gale Academic OneFile, <https://link.gale.com/apps/doc/A476905245/AONE?u=jrycal5&sid=AONE&xid=dcefd440>.
- Rauchs, M., A. Blandin, K. Klein, G. C. Pieters, M. Recanatini, and B. Z. Zhang. 2018. "2nd Global Cryptoasset Benchmarking Study." Available at SSRN 3306125.
- Rizzo, P. 2017. "8-Hour Miner Meeting Ends with Litecoin Scaling Agreement." Coindesk, 21st April.
- Shin, L. 2015. Bitcoin's Shared Ledger Technology: Money's New Operating System." Forbes, September 28. Available at: <https://www.forbes.com/sites/laurashin/2015/09/09/bitcoins-shared-ledger-technology-moneys-new-operating-system>.
- Soska, K., and N. Christin 2015. "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem." Paper presented at the USENIX Security Symposium 2015.
- Statista 2019. "Worldwide Blockchain Users." <https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/>.

- Swan, M. 2015. *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O'Reilly.
- Swanson, T. 2015. "Consensus-as-a-Service: A brief report on the emergence of permissioned." Distributed Ledger Systems. <https://www.ofnumbers.com/2015/04/06/consensus-as-a-service-a-brief-report-on-the-emergence-of-permissioned-distributed-ledger-systems/>.
- Szabo, N. 2008. "Bit Gold." *Website/Blog*.
- 1997. "The God Protocols, Satoshi Nakamoto Institute." Available at <https://nakamotoinstitute.org/the-god-protocols/>.
- 1998. "Secure Property Titles with Owner Authority, Satoshi Nakamoto Institute." Available at <http://nakamotoinstitute.org/secure-property-titles/>.
- 2002. "Shelling Out: The Origins of Money." Altruists.Org/F40. <http://nakamotoinstitute.org/the-god-protocols/>.
- Tarasiewicz, M., and A. Newman. 2015. "Cryptocurrencies as distributed community experiments." In D. L. K. Chuen (ed.), *Handbook of Digital Currency*, Elsevier, Chapter 10, 201–222.
- The Economist 2017. "The Magic of Mining," 8th January.
- Tindell, K. 2013. "Geeks Love the Bitcoin Phenomenon Like They Loved the Internet in 1995." 5th April, Available at <http://www.businessinsider.com/how-bitcoins-are-mined-and-used-2013-4?IR=T>.
- Weber, B. 2016. "Bitcoin and the legitimacy crisis of money." *Cambridge Journal of Economics* 40:1, 17–41.
- Williams, S. 2016. "Decentralization is Disrupting Vertical Industries, Digital Finance News." 19th January, Available at <https://digitalfinancenews.com/index.php/2016/01/19/decentralization-is-disrupting-vertical-industries/>.
- Wood, G., and A. Buchanan. 2015. "Advancing Egalitarianism." In D. L. K. Chuen (ed.), *Handbook of Digital Currency*, Elsevier, Chapter 19, 385–402.
- Yermack, D. 2015. "Is Bitcoin a Real Currency? An Economic Appraisal." In D. L. K. Chuen (ed.), *Handbook of Digital Currency*, Amsterdam: Elsevier. Chapter 2, 31–43.
- 2017. "Corporate governance and blockchains." *Review of Finance* 21, 7–31.