Junior Management Science

journal homepage: www.jums.academy

The State of the Art in Cryptocurrencies

Yasmin Le

Universität Mannheim

Abstract

Bitcoin has emerged as a popular digital currency and arouses the interest not only of programmers, but also of investors and academics. What interests them most is its underlying technology, the blockchain. This thesis aims at giving an overview of the current state of cryptocurrencies and compares their different designs and approaches to Bitcoin. The blockchain technology will be explained, as well as how it could impact many aspects in life by showcasing different applications of Ethereum blockchain-based smart contracts. Based on the evaluation of the different cryptocurrencies and preceding conclusions, specific cryptocurrencies will be applied to the Tasklet system before proposing the implementation of the blockchain technology in such a system, in order to establish a reward system.

The paper reviews a heterogeneous, scattered body of knowledge including academic literature, but also non-scientific sources due to the constantly evolving technology. On this basis, the advantages of Bitcoin, but also its weaknesses, as well as the vast potential of blockchain are discussed. Results indicate that although Bitcoin's framework may be limited, it will still play an important role in the future due to its dominance in the cryptocurrency market. The short display of blockchain-fueled applications and its effects has shown its potential to transform the internet, leading to the rise of the Web 3.0.

Keywords: Bitcoin, Blockchain, Cryptocurrency, Distributed Ledger Technology, Smart Contract

1. Introduction

Already in the 1980's, the idea of cryptocurrencies existed when the first proposal for "untraceable payments" was made by Chaum in 1983 (Chaum (1983)). Since then, many ongoing improvements and extensions have been suggested. However, these early attempts lack proper security mechanisms against cyberattacks and still require a central authority as a controlling instance. With the introduction of Bitcoin in 2009, these difficulties were finally overcome, as it provides a decentralized network for secure transactions (Tschorsch and Scheuermann (2016)). Bitcoin has emerged as a popular digital currency and arouses the interest not only of programmers, but also of investors and academics. What interests them most is its underlying technology, the blockchain.

Blockchain enables a distributed peer-to-peer network where no trusted party is required anymore. Based on this technology, many alternative currencies have emerged, aiming to solve some of Bitcoin's weaknesses (Bonneau et al. (2015)). However, blockchain's impact goes far beyond currency. It allows for self-enforcing contracts, so-called smart contracts, automating complex multi-step processes (Christidis and Devetsikiotis (2016)). These contracts are run by networks like Ethereum and enable various applications in many areas. The potential of blockchain will drive innovation, leading to more efficiency and democracy in existing systems and organizations (**?**). Since the technology surrounding cryptocurrencies and blockchain is constantly evolving, this paper also relies on wikis, forums, blogs and other non-scientific sources.

1.1. Objective of the Thesis

This thesis aims at giving an overview of the current state of cryptocurrencies and compares their different designs and approaches to Bitcoin. Given Bitcoin's prominence, the paper will pay special attention to Bitcoin and evaluate its design with focus on its underlying technology, the blockchain. In order to demonstrate the scope of the technology and how it could impact many aspects in life, different applications of Ethereum blockchain-based smart contracts will be showcased. Based on the evaluation of the different cryptocurrencies and preceding conclusions, specific cryptocurrencies will be applied to the Tasklet system in order to propose the most suitable one for supporting a payment system in this real use case.

DOI: http://dx.doi.org/10.5282/jums/v2i3pp1-10

1.2. Structure of the Thesis

The paper is organized as follows. First, key concepts of cryptocurrencies are outlined and Bitcoin is introduced. Chapter 3 examines Bitcoin's protocol and structure. Technical challenges and limitations of Bitcoin are also addressed, for which solution approaches in the form of alternative cryptocurrencies will be reviewed in Chapter 4. The implications of having blockchain as a basis technology and its vast potential are discussed, before proposing, in Chapter 5, its implementation in a Tasklet system to establish a reward system. Finally, Chapter 6 concludes this thesis with a brief summary and outlook for future development.

2. Theoretical Foundations

This chapter introduces important terms and key concepts which lay the technical foundations for cryptocurrencies. A brief introduction to Bitcoin will be given and, in a second part, its underlying technology, cryptography, will be explained.

2.1. Bitcoin

In 2008, the anonymous group or person, Satoshi Nakamoto, introduced the cryptocurrency Bitcoin in (Nakamoto (2008)). However, the idea of a digital currency dates back to the 1980's. Unlike Bitcoin, all these early attempts required a central authority (Tschorsch and Scheuermann (2016)). In later stages, the proof-of-work (POW) puzzles were proposed to fulfill the function of money supply independently from banks. Still, the fundamental problem of double-spending could not be solved until Bitcoin was designed. Bitcoin uses already existing encryption algorithms and combines them in a new way to ensure secure transactions. Its main goal is to provide a decentralized system without the need of a third party to regulate transactions. There is no trust requirement; instead, Bitcoin relies solely on cryptographic proof. Thus, Bitcoin is based on a peer-to-peer (P2P) network using POW (Nakamoto (2008)). The core of the Bitcoin protocol is the blockchain technology, which serves as a distributed ledger, collecting all the information on transactions ever made (Tschorsch and Scheuermann (2016)). This results in complete transparency, since all transactions are publicly visible to the network.

2.2. Underlying Technology

Before going more deeply into the Bitcoin protocol, Bitcoin's basic concepts will be explained. Bitcoin is based on cryptography, which might be surprising at first because it is a currency and not a tool for sending secret codes (Nielsen). However, Bitcoin aims to ensure the security of transactions, which can be achieved through a cryptographic protocol. To understand how cryptocurrencies function, a basic sense of cryptographic primitives is necessary. Below, hash functions and public key cryptography will be explained along with applications in building cryptocurrencies.

2.2.1. Cryptographic Hash Function

A hash function is a mathematical function which can take any data of arbitrary size as input, called messages. Its output results in the same value for the same message and always has a fixed size. Outputs are also called message digests or hash (Silva (2003)). Hash functions are one-way functions, i.e. by only knowing the output, it is infeasible to determine the input. Cryptographic hash functions differ from regular functions in specific properties, of which three will be further elaborated on.

Properties. To be secure, cryptographic hash functions have to be defined by three particular properties. First, the function has to be collision-free. It should be difficult to find two different messages that produce the same hash value. A collision occurs when two different messages produce the same hash. The longer the hash, the less probable a collision will occur, due to the increased number of possible values when having more bits. Secondly, it has to be hiding. When given the output of a hash function, it should be difficult to find out the initial input. An attacker will not be able to determine the original message by only knowing the hash. Since different messages almost always produce different outputs, a file changes if its message digest does (Silva (2003)).

Application. Cryptographic hash functions are used to provide data integrity and authentication when verifying the integrity of files or passwords. Bitcoin uses the functions, called SHA-256, for POW in their mining process. A general illustration of their application (cf. Figure 1) is as follows. Alice provides Bob with a puzzle and claims to know its answer. Bob wants to solve it, but also wants to be sure that Alice is telling the truth. Hence, Alice computes the hash of the solution and tells Bob its hash value. Now, Bob can solve the puzzle himself. After that, he can compare his solution to Alice's by hashing it and checking if it matches Alice's hash value.

2.2.2. Public Key Cryptography

Bitcoin uses public key cryptography, in which it applies asymmetric cryptography and mathematically related pairs of keys. There are two types of keys: public keys, known to a wide audience, and private keys, only known by the owner. This leads to authentication when verifying that the message was sent by a holder of the paired private key by using the public key. It also enables encryption, because only by having the paired private key can the message be decrypted, and provides security (IBM (2017a)). The most common forms of application are described hereafter.

Public Key Encryption. Any person can encrypt a message with the public key, but only the holder of the paired private key can decrypt the message (cf. Figure 2). Thus, asymmetric key algorithms are used. The same key cannot be used for both encryption and decryption. Instead, the keys of each pair are used to reverse the work done by the other (IBM (2017a)).

Digital Signatures. They basically function as signatures on paper. This means only one particular can make their signature, but anyone who sees it can verify the validity of their identity. For digital signatures, a message is signed with the private key of the sender, but anyone who has access to the matching public key can verify it. To create a digital signature, the document first has to be distilled into a large number, the digest code. Then, this code gets encrypted with the private key resulting in the digital signature, which is bound to that particular document. Now, if the message changed slightly, the digest code would also change. Hence, verification would fail for any other message, no matter how trivial the difference to the original message is. When the recipient receives the message, he has to recompute the digest code for it. To decrypt the signature, the public key has to be used, resulting in the original digest code. Then the recipient has to compare the recomputed digest code with the original one. Only if both match is the message intact and authentic (IBM (2017b)).

3. Bitcoin Technologies

After having laid the foundation, the Bitcoin protocol will be described and analyzed as originally introduced in (Nakamoto (2008)). This chapter presents a basic view on digital currencies and explains them in more detail later. Thereby, the characteristics of Bitcoin as well as the blockchain technology and how this technology enables Bitcoin to solve several problems will be illustrated. Furthermore, the chapter addresses possible problems and weaknesses of Bitcoin regarding the five key issues.

3.1. Blockchain

Often, transactions are regulated by a third party, leading to transaction costs, since the intermediaries want to be compensated for their services. For example, Alice wants to transfer coins to Bob; in order to ensure the validity of the transaction, the coins must be clearly identifiable (Tschorsch and Scheuermann (2016)), i.e. every coin receives an unique number; but these numbers have to be issued from a trusted source, i.e. a bank; the bank maintains the ledger and updates it continuously. Bitcoins aims to get rid of such a centralized authority by using the blockchain technology (cf. Figure 3).

Blockchain builds the core of the Bitcoin protocol. Its first and also most common application is Bitcoin, for which it serves as the distributed ledger, including all past transactions chronologically. Thus, the growing list of transactions is constantly updated and made publicly available to all nodes, together with Bitcoin's transaction history. Through blockchain a trusted third party is not required anymore and, thus, decentralization is established. Not only transparency can be reached by that, but also anonymity, increasing the security for other nodes to confirm transactions. Once the transaction has been verified by all nodes, it is tamper-proof. This results in high security of transactions (Yli-Huumo et al. (2016)). However, Bitcoin still faces some challenges.

Double-Spending. Alice could be tempted to redeem some transaction input in two separate transactions, sent to two different receivers, Bob and Carol (Bonneau et al. (2015)). Looking at the transactions separately, Bob and Carol could verify and accept their transaction, which leaves the blockchain inconsistent. Bitcoin overcomes double-spending by demanding that transactions must be made public in a P2P network, so that all participants can verify the transaction validity (Tschorsch and Scheuermann (2016)). It should be accepted only if the majority agrees on the validity of a transaction. Then it is collected into a block, while each of these blocks contains a timestamp and the hash of the previous block. Hence, a specific order is established, resulting in the so-called blockchain.

Sybil attacks Another problem arises through Sybil attacks: Alice sets up multiple entities, making up the majority of the network, to confirm her transactions; she can then still double-spend her coins and cheat on the system; both Bob and Carol would trust the verification of the network and accept the transaction (Tschorsch and Scheuermann (2016)).

3.2. Mining

To prevent these attacks, Bitcoin uses the POW concept in its mining process, during which, new transactions are broadcast to every node in the network (Nakamoto (2008)). The miners, the network participants, compete against each other trying to solve a puzzle, the POW. The first to solve the POW broadcasts the block in the network, and after its verification the block is added to the blockchain. Solving the puzzle is computationally challenging and requires high computational power. Therefore, the increasing number of identities, and thus multiple votes, do not guarantee (seizing) control over the system (Tschorsch and Scheuermann (2016)) and the problem of Sybil attacks can be avoided.

Proof-of-Work. The POW requires finding a hash with a value less than or equal to a specific target value (Tschorsch and Scheuermann (2016)), which influences the puzzle difficulty. Due to the randomized character of the puzzle, the share of computational power (CP) is always equal to the chance of solving the POW. About every 10 min a new block is verified. To maintain this, the target value is adjusted every 2,016 blocks (Bonneau et al. (2015)).

Calculating the hash requires high CP, i.e. energy and money. Hence, it may not be immediately apparent what incentivizes miners to compete in this race. Mining not only has the function of verifying transactions, it also increases the Bitcoin upply. The first miner to solve a block receives a Bitcoin reward of a certain amount, which is currently 12.5 Bitcoins (BTC) for every block. Initially, a block reward of 50 BTC was given out. Since then, the generation of BTCs is halved every four years until it is below 10^{-8} BTC, a satoshi, the minimal unit of Bitcoin (Tschorsch and Scheuermann (2016)).

Since each block contains a pointer to the prior block, a linear chain is formed and a total block order is established. However, it is possible that temporary forks occur: by chance, two miners provide two different valid solutions almost simultaneously for the same block. Then consensus is broken, since miners can choose either fork to work on. Bitcoin is designed to resolve these forks by always following the longest fork, so that only one chain branch survives (Tschorsch and Scheuermann (2016)). Thus, consensus is restored. The longest version is always the consensus blockchain (Bonneau et al. (2015)), which is the one expected to be most difficult to produce and not the one with the most blocks. Hence, attempts to create the longest fork by splitting the chain and then creating many simple blocks are prevented (Wood (2014)). The orphaned (abandoned) fork (Tschorsch and Scheuermann (2016)) and all its transactions are considered invalid. All in all, a transaction is only verified if it is part of a block in the longest fork and it has six successive block confirmations.

3.3. Transactions

Transactions transfer currency from one user to another (Bonneau et al. (2015)) and assign ownership rights. The growing transactions are the only state in Bitcoin. Coins per se do not exist.

Every transaction needs a virtual wallet with at least a publicprivate key pair. The public key derives address (Tschorsch and Scheuermann (2016)) using SHA-256, whereas the private key proves ownership over certain outputs. Outputs and inputs are contained in every transaction. Each output represents a fraction of the Bitcoin currency and contains a short code snippet. It defines the conditions under which this transaction output can be redeemed (Bonneau et al. (2015)). Each input always refers to the previous transaction, enabling every transaction along the blockchain to be tracked. Thus, the user will either arrive at the first Bitcoin transaction or coinbase transaction. These transactions are special, as they only include outputs. When arriving at the first Bitcoin transaction, the genesis block will be reached. Every block, except for the genesis block, includes a record of which addresses or scripts will receive the reward. This record is called a coinbase transaction and responsible for introducing new currency units into the system. For every standard transaction, the sum of all inputs must be equal to or greater than the sum of all outputs. If the input is greater than the output, the difference has to be included in a transaction fee to the miner who was working on the respective block (Tschorsch and Scheuermann (2016)).

3.4. Challenges and Limitations of Bitcoin

Although Bitcoin offers many benefits, the currency struggles with technical deficiencies and limitations. Applying Bitcoin can entail major risks and work as a double-edged sword. Often, Bitcoin is associated with illegal activities. One prominent example is its role behind the online drug market Silk Road (Pagliery (2013)). Through anonymity and decentralization Silk Road could operate money laundering, while hiding actors' identities. Not only since this incident, but also because Bitcoin has become more mainstream, institutions and governments have shown growing concerns regarding regulating issues, such as taxation. Even users partly criticized Bitcoin for its privacy or security issues. In the following, the paper will discuss five key challenges for Bitcoin: network capacity, latency, security, wasted resources, and privacy according to (Yli-Huumo et al. (2016)). The focus will mainly be on technical aspects.

Network capacity. Bitcoin's popularity has grown since its launch in 2009, which can be observed by the constantly growing number of Bitcoin transactions. Within two years, the number of transactions has more than tripled (Blockchain.info (2017)) and it is even predicted to rise again. Bitcoin might face difficulties processing more transactions if it does not improve its network capacity. Compared to VISA, which can process 2000 transactions per second (tps), Bitcoin is currently only able to process a max. of 7 tps (Yli-Huumo et al. (2016)). Becoming more popular, its throughput level has to increase to similar levels. However, with this improvement new problems arise. Roughly every 10 min a new block with a size of 1 MB is created. Bitcoin's current blockchain size is already 113,530 MB (Blockchain.info) and with increasing transactions it will grow even further. Thus, size and bandwidth issues have to be addressed.

Latency. Consensus, ergo a block verification, is designed to take 10 min for security reasons and to detect double-spending attacks. But to be "deep" enough in the ledger so that forks are unlikely to occur anymore, another one to two hours have to be considered. This delay poses a vulnerability of the protocol, since an initially verified transaction might be nullified later, when it becomes part of the orphaned fork. Latency also impedes Bitcoin in competing with other payment systems for fast-paced transactions, e.g. financial trading (Berke (2017)). Therefore, many users prefer zero-confirmation transactions, which can propagate between users within seconds, but hold a higher risk of double-spending attacks (Karame et al. (2012)).

Security. The most concerning issue Bitcoin faces is security. Exceeding a market value of $2,000 (CoinMarketCap (2017)), profit-oriented attacks on the system are innumerable. Not only double-spending poses a threat, Distributed Denial-of-Service (DDoS) attacks and other issues are also challenging Bitcoin. However, the most prominent problem are 51%-attacks, attempts to dominate mining power.

Security Incidents. With the increasing value of Bitcoin, the number of thefts has also increased. This is not a failure of Bitcoin's security, but a consequence of its reliance on PKC for user authentication. The private key is the main authentication element. If it gets stolen or lost, all stored coins are lost, too. Hence, thefts are owed to insecure storage (Berke (2017)). Due to the rising difficulty of solving POWs, miners join mining pools, combining their hashing power to verify transactions and then distribute the reward. Particularly large pools are targeted by DDoS attacks, attempts to disrupt online service by overwhelming it with traffic from multiple sources.

51%-attacks. As more and more CP concentrates in a few large mining pools, the risk of 51%-attack increases. This is problematic because the entity controlling the majority of the power could manipulate the blockchain and solve their own block of transactions (Bradbury (2013)). And even if a single pool does not exceed the 50% mark by itself, coalitions could. They act like a cartel, releasing or keeping information as they please. Miners can establish a private chain when not broadcasting their blocks. As soon as the public chain approaches the private chain's length, the rogue miner announces his private blocks to catch up. Due to this propagation delay, blockchain forks are intentionally caused to gain an advantage on winning subsequent blocks. Thus, miners earn a higher revenue than their fair share by letting the others waste their power mining on the public chain. This strategy is called selfish mining. Another harming strategy is temporary block withholding which enables double- spending. Again, the pre-mined blocks are kept secret and for each of them the miner includes a self-payment, i.e. the double-spend transaction, by initiating a transaction referring to the same coins, which will be considered as valid by the network. As soon as the trade is completed, the pre-mined block with the double-spend is broadcast. Thus, market-based centralization of mining power in pools creates longer transaction approval time and facilitates double-spending (Tschorsch and Scheuermann (2016), Eyal and Sirer (2014)).

High Computational Power. Through Bitcoin's increasingly difficult mining process, another issue has emerged: high energy consumption, which was comparable to Ireland's total electricity consumption in 2014. In this process, limiting factors are the hash rate of hardware and the running cost. Initially, mining took place on regular computers. However, as Bitcoin gained prominence, a computation race between miners has begun, in the effort to increase their hash rate. Currently, Application Specific Integrated Circuits (ASIC) are used to perform the Bitcoin hash at higher rates while lowering the energy necessary (O'Dwyer and Malone (2014)).

Privacy. Although a market place like Silk Road would not be possible without Bitcoin, privacy was never the main goal of the protocol. Bitcoin only offers a limited form of unlinkability by allowing users to create new addresses (pseudonyms) at any time. Due to Bitcoin's transparent nature, it is possible to trace transactions between addresses and link them to IP addresses, where the transaction is generated (Bonneau et al. (2015), Tschorsch and Scheuermann (2016)). Information about users can be obtained by the P2P network (Reid and Harrigan (2013)). Usually, a miner is connected to eight peers, called the client's entry nodes, and broadcasts their addresses to the network. These addresses can be mapped to an IP address simply by observing the Bitcoin flow (Biryukov et al. (2014)).

4. Alternatives Cryptocurrencies

This chapter discusses proposed changes to Bitcoin. Different solution approaches towards the preceding problems will be presented, including alternative digital currencies and protocols. In doing so, the paper will evaluate and compare them to Bitcoin. Lastly, it introduces the newly established altchain Ethereum and demonstrates its potential for various applications. Closely related to it, the blockchain technology and its impact beyond Bitcoin will be further elaborated on.

4.1. Modifying Bitcoin

Because changes and extensions to Bitcoin are limited, alternative approaches result in new currencies – so-called altcoins. Over 800 cryptocurrencies currently exist, such as Bitcoin, Litecoin and Dash (CoinMarketCap (2017)). The majority of these currencies is very similar to Bitcoin in that they have been created by forking Bitcoin's protocol and rely on its main features. However, some currencies have a fully different design (Bonneau et al. (2015)). Altcoins were mainly created to fix shortcomings of Bitcoin, whereby certain changes only attract smaller groups while others appeal to a wider clientele and can be regarded as a real competition to Bitcoin. Instead of suggesting upgrades for Bitcoin itself, this section focuses on the two most popular altcoins regarding market capitalization and largest improvements.

4.1.1. Litecoin

The creation of Litecoin in 2011 was never intended to replace Bitcoin, but rather to serve as the silver to Bitcoin's gold (Xie (2017)). Since then it retained its position among the top five cryptocurrencies (Gandal and Halaburda (2014)). Its popularity mainly stems from its faster transaction times and mining improvements. Bitcoin sets the incentive to use powerful specialized hardware in the network, which is costly. Thus, not everyone can participate in mining. Litecoin wants to allow everyone to access and participate in this process. Therefore, a more memory-intensive mining algorithm was introduced, making it resistant to specialized hardware mining technologies such as ASIC. Instead of using Bitcoin's SHA-256 algorithm, Litecoin is based on the more memory-intensive Scrypt POW algorithm. With a faster transaction time, Litecoin is able to process a higher volume of transactions. Instead of 10 min it needs 2.5 min, a quarter of the time Bitcoin needs. Thus, Litecoin is able to supply a quadruple amount of Bitcoin's total coin supply (Xie (2017), Litecoin (2017)).

4.1.2. Ripple

In 2012, the decentralized IOU (I Owe You) credit network Ripple was established. Its prominence as a fast and low-cost cryptocurrency has risen since. To comprehend this phenomenon, Ripple's technology and special features have to be examined first. Considering the importance of understanding how Ripple differs from Bitcoin, the paper will also draw comparisons to Bitcoin.

Ripple is at its core a distributed-consensus ledger. Every transaction is recorded in real-time, and it automatically updates changes in any of the users' assets. Thus, its entire transaction history can be tracked, similar to Bitcoin's. When changes are made to the ledger, the change is processed by the Ripple Protocol Consensus Algorithm (RPCA). Meanwhile the network servers will mutually agree to the change and apply this to their ledger copy. Ripple introduces a new component, the Unique Node List (UNL) (Tasca (2015)), which is maintained by each server s and will be queried when determining consensus. The UNL contains a set of servers other than s. Only their votes count when determining consensus, contrary to Bitcoin's network, which considers every node. Hence, the UNL represents a subset of the network, which can be "trusted" by s to not engage in fraudulent activities, when taken collectively (Schwartz et al. (2014)). Consequently, forks are prevented. Further, RPCA provides the benefit of lower energy costs, since it is not based on miners or a POW scheme.

Ripple only exchanges and transfers IOU currency within its network. Thus, users are required to exchange their assets in IOUs via gateways first. A gateway is a prominent wallet and trusted by several wallets in the system to create and maintain a credit path correctly. Usually, they are widely connected nodes and, thus, the created credit path enables the new wallet to interact with the rest of the network. Ripple executes transactions only if a credit path exists between the users with enough IOU credits, whereas Bitcoin allows any two users to exchange BTCs via a direct payment between them. By only working with IOU currency, Ripple has a competitive advantage over Bitcoin. It can provide settlement solutions for various types of assets: Bitcoin and other cryptocurrencies, fiat currencies, or commodities. In fact, it is capable of monetizing everything as long as both parties of the transaction trust each other in terms of IOUs they are willing to extend to each other. Therefore, Ripple can process two transaction types. The first type is a direct XRP (Ripple) payment, for which a wallet needs to contain a certain amount of XRP and a small transaction fee in XRP has to be paid by the issuer. Between these payments no credit path is necessary. The second type is a path-based settlement transaction and is used when having other currencies than XRP. Ripple distinguishes three kinds of currencies – fiat, cryptographic, and user-defined currencies - which are all treated equally. Further, exchange wallets exist that receive a certain currency in one of their links and exchange it for another currency in another link. This enables cross-border payments, while not depending on a highly-volatile underlying coin (Moreno-Sanchez et al. (2016)).

Looking at the above benefits, Ripple's prominence and attraction for many financial institutes become evident. Banks join Ripple's global transaction network to facilitate real-time cross-border payments without any uncertainty, no settlement risk and complete traceability. This results in new opportunities, enabling Ripple's main goal: the rise of the Internet of Value (Tasca (2015), Ripple (2017)).

4.2. Alternative Extensions

Many extensions have been proposed to solve some particular perceived problems with Bitcoin. CoinJoin, for instance, addresses the issue of privacy by enhancing it through multi-signature transactions (Tschorsch and Scheuermann (2016)). However, this section will focus on the extension Zerocoin, which also aims at fixing privacy issues of Bitcoin.
Zerocoin. Zerocoin is a distributed e-cash system that upgrades the Bitcoin protocol to ensure complete anonymous transactions without adding trusted parties (Miers et al. (2013)). In doing so, it solves one of Bitcoin's main weaknesses: anonymity.

When using Bitcoin, user privacy could only be enhanced by employing multiple pseudonyms. Nevertheless, the de-anonymization of individuals is still possible with information from the public ledger. Thus, Bitcoin fails to guarantee privacy, whereas Zerocoin solves this issue by applying zero-knowledge proofs to inhibit transaction graph analyses. Unlike Bitcoin, it does not use digital signatures for authentication. Instead, it can rely on proving that the coins belong to a public list of valid coins (Ben-Sasson et al. (2014)). This works as follows: Alice produces a secure commitment scheme, i.e. the zerocoin; the zerocoin is then recorded in the blockchain, so that all users can verify it, given its correctness in sum of currency and structure; next, she broadcasts a non-interactive zero-knowledge proof for the respective zerocoin, along with a "spend" transaction; the remaining users check transaction and proof; only if they are secure do users allow Alice to collect the currency amount. This way, the system ensures unlinkability by using Bitcoin as the backing currency and zerocoins as an anonymous shadow currency (Miers et al. (2013)). Transactions are only in the base currency. However, users can convert the base currency into and out of zerocoins (Bonneau et al. (2015)).

Although Zerocoin provides an alternative privacy-enhancing approach, it lacks in performance and functionality. For these reasons, daily routine transactions still have to be carried out with Bitcoin. Performance-wise, Zerocoin is computationally complex and requires more storage in the ledger. Thus, the entailed costs are higher than for Bitcoin. Functionality-wise, Zerocoin requires protocol modifications for full-fledged anonymous payments. It uses coins of fixed denomination, i.e. it neither supports payments of exact values, nor transactions for change. Even though Zerocoin ensures anonymity by unlinking a transaction from its origin, it still reveals destinations and transaction amounts (Ben-Sasson et al. (2014)).

4.3. Altchains

Apart from the aforestated altcoins, another alternative to Bitcoin are altchains. They implement a new structure with Turing-complete stack language, through which the creation of smart contracts is enabled. Via smart contracts, terms of contracts agreed by users to applications such as sharing resources can be executed (Wood (2014)). This section will concentrate on the most promising altchain, Ethereum.

4.3.1. Ethereum

Ethereum (Ethereum) is an open-source project, built on a blockchain-based platform, which enables developers to create and use decentralized applications, such as smart contracts. Smart contracts are "a set of promises, specified in digital form, including protocols within which the parties perform on these promises" (Szabo (1996)). Being deployed on a blockchain, they are executed as programmed without the risk of censorship, downtime, fraud, or third-party interference. Although no such system was established 30 years ago, the importance of algorithmic enforcement of contracts was realized and it was proposed that they would have a huge impact on the future of law. Hence Ethereum may be regarded as such a crypto-law system (Wood (2014)).

Ethereum Virtual Machine. At Ethereum's core is the Ethereum Virtual Machine (EVM), which "forms the key part of the execution model for an Account's associated EVM Code" (Wood (2014)) and is Turing-complete. By using a Turin- complete scripting language, any user can add their own application on top of the blockchain. These applications are also called Dapps, which stands for decentralized applications. Indeed, there is no single point of control or failure, since decentralization enables more efficiency, scalability and resilience to attacks. Often, Ethereum is also called a "global singleton computer" because every node of its P2P network runs the EVM to maintain decentralized consensus, and performs the same instructions. The Ethereum platform itself is neutral and featureless, allowing developers to use it for whatever they wish. However, some applications are more suitable than others. Dapps with automated direct interaction between peers or which facilitate coordinated group action benefit the most from the system (The Homestead Documentation Initiative).

Ethereum Accounts. Many technical components of Bitcoin are also implemented by Ethereum. However, it also features own extensions and innovations. In Ethereum, so-called accounts define the state with state transitions, which directly transfer value and information between accounts. Two types of accounts exist: externally owned accounts (EOA) and contract accounts. EOAs have no code, as they are controlled by private keys. Hence, whoever holds the private key also controls the EOA. Contract accounts are controlled by their contract code. When the contract account receives a message, its code gets activated. Thus, it can read and write to internal storage, send other messages, or create contracts in turn (Buterin (2014)).

Transactions. For every transaction, users have to pay a fee to prevent DDoS attacks. Ethereum's native value-token is Ether (ETH), but the fee is paid in Gas, "the fundamental network cost unit. Paid for exclusively by Ether [. . .], which is converted freely to and from Gas as required." (Wood (2014)). In order to protect Ethereum from infinite loops or other malicious computational tasks, each transaction needs to limit the steps number in computation that it can use to execute the code. The fee system intends to oblige an attacker to pay in proportion to his consumption of resources (Buterin (2014)). As with Bitcoin, Ethereum's mining process is based on POW. However, it works slightly differently by using a memory-hard POW, the Ethash. Instead of only requiring computational power, memory as well as CPU are required, making the ideal hardware a general computer (Wood (2014), The Homestead Documentation Initiative). Thus, Ethereum makes the POW ASIC-resistant and, by that, it solves Bitcoin's centralization problem. This, in turn, gives everyone fair access to this resource, since Ethereum can be used wherever there is internet.

Comparison to Bitcoin. By additionally using basic programming languages such as JavaScript, Ethereum is more accessible to developers than Bitcoin. Besides, Ethereum overhauls Bitcoin in many other aspects, such as a shorter verification time and a smaller block size (Lewis). However, most important is its allowance for smart contracts. Whereas Bitcoin only serves as a digital currency, Ethereum also enables various applications, from financial to e-governance. This makes its potential so vast and a driver of innovation. Therefore, the next section will explore Dapps and the potential of its underlying technology, the blockchain, beyond Bitcoin.

4.3.2. Applications of Ethereum and the Potential of Blockchain Technology

Dapps. Ethereum provides a platform for zero-trust computing smart contracts, permissions management, autonomous trading, and many more applications. Dapps can be categorized into three types: [1] financial applications, such as financial derivatives; [2] semi-financial; and [3] nonmonetary; e.g. online-voting. Table 1 provides an extended overview of Dapps. However, this section will focus on the most prominent applications on top of Ethereum (Buterin (2014)).

The most common application of smart contracts are financial ones. Benefits of Ethereum are the possibility to value positions for real-time monitoring, while avoiding information leakage and reducing risk of fraud or cyberattacks; but also automated settlement of agreements, while executing pre-defined tasks. Thus, smart contracts enforce a standard set of rules to transactions and thereby optimize the derivative trade. Most importantly, it decreases time on deal closings and other transactions (Alliance (2016)).

However, not only the finance sector profits from Ethereum; also the entertainment industry is interested in the technology, as the recent acquisition by Spotify of the startup Mediachain Labs, which runs on Ethereum, proves. Spotify faces difficulties in obtaining mechanical licenses and allocating royalty payments (Perez). Through smart contracts, profits are ensured to go back to the artist and they can share free-trade music. They even might be able to sell their music directly to consumers without relying on intermediaries. Ethereum takes this idea even further and introduces the concept of Decentralized Autonomous Organizations (DAO). They are virtual entities which allow the majority of their members to decide about their funds and modify their code. Since smart contracts set terms of ownership and allocation of funds, managers or lawyers will not be needed anymore to run a company. Therefore, Ethereum facilitates the management of companies.

Relying more and more on the internet and online services, such as online banking or social media, users have no choice but to provide private information, often without knowing what happens to their data. Smart contracts provide decentralized identity management systems, where individuals are in full control of their digital identity and reputation. For a contract, all data is stored inside the Ethereum network and can only be modified or removed by the particular individual. This data could then be accessed by other contracts through function clauses (Buterin (2014)).

Potential of Blockchain. The third chapter explained how blockchain functions, whereby the emphasis was on its most common application, Bitcoin. However, there is more to blockchain than being the basis of cryptocurrencies. All the preceding applications are enabled by smart contracts and they, in turn, only function due to the blockchain technology. In fact, blockchain is evolving in many ecosystems, e.g. Ethereum and Hyperledger. Thus, blockchain needs an integration solution, through which, for instance, a transaction on Hyperledger could access information from Ethereum and vice versa. The potential of blockchain is immense, considering that it enables the democratization of the internet and other services through smart contracts. Thus, blockchain acts as a middleman that executes legal obligations, business deals, and data exchanges (Marvin (2017)). However, blockchain has also the potential to solve urgent problems in developing countries, where often there is no access to proper land titling. Land titles could be stored on the chain, creating more transparency. Thus, people would gain access to credits as they can prove authenticity of title claims (Underwood (2016), Dahan and Casey (2017)).

To conclude, blockchain has the potential to disrupt established industries and drive innovation in various areas. By providing decentralized, open and trustless platforms, blockchain-based ecosystems like Ethereum coined the term Web 3.0. It is an umbrella term associated with connective intelligence and "An internet where core services like [. . .] digital identity are decentralized, and where individuals can engage in economic interactions with each other." (The Homestead Documentation Initiative). One of these interactions is cloud computing, an application which allows users to rent out spare CP and ask others to execute computations. How this application can be relevant for a specific computing system will be addressed in the next chapter.

5. A Real Case Application of the Blockchain Technology

This chapter introduces the research project TASKLETS and discusses how blockchain can enhance features of the Tasklet system. Different proposals on which cryptocurrency and its design apply best to facilitate an individualized payment system within the Tasklet system will also be given.

5.1. Tasklet Systems

TASKLETS aimed at developing a distributed computing system. Such a system could serve as an alternative to powerful specialized hardware, which is costly. Often, CP of individual users remains unused. This spare resource could be shared within a distributed network and then utilized by other computation-intense applications. Tasklet systems (TS) as introduced in Schäfer et al. (2016a) build a framework for such networks. They enable interoperability in heterogeneous computing sources and enhance the execution of computationally intensive applications.

Tasklets are extracted subroutines of these applications, operating multiple different processing entities. TS consist of three different entities. While providers offer their resources in form of virtual machines to resource consumers that require additional CP, a broker oversees this process by scheduling and matchmaking. In this process, Tasklets are exchanged directly between the two parties in a P2P network (Schäfer et al. (2016b)). To incentivize providers to offer their computational resources to the network, a reward system needs to be implemented, which needs to facilitate payments between consumers and providers. In the following, possible solutions and systems with monetization mechanisms similar to TS will be discussed.

5.2. Implementation of Cryptocurrencies

Since altcoins are based on a distributed ledger, they would make the perfect remuneration tool in TS. The blockchain technology enables decentralization and scalability. By applying the technology to the system, there would be no need for a trusted authority and no single point of failure, even though the system is connecting many entities in a P2P network. Through blockchain, the TS could therefore implement an appropriate monetization mechanism. Because the exchange medium is not only money, but also CP, Bitcoin-like currencies do not qualify as appropriate remuneration systems. They are only designed as a digital currency, when actually a transaction network that facilitates settlement solutions for various assets is required. Therefore, possible supporting systems could be Ripple or Ethereum.

5.2.1. Ripple as a Remuneration System

Considering that Ripple only exchanges in IOU currency and thus enables payment solutions for different assets, it could serve as the underlying structure for a remuneration system in TS. Ripple allows the monetization of everything as long as the two connected Ripple wallets of the transaction trust each other in terms of IOUs they are willing to extend each other. In the TS, each of the participating devices' ledgers could be linked by Ripple Connect through the neutral Interledger Protocol (ILP) for the cross-border payment settlements. Since ILP can work with any new system, Ripple could serve as an user-defined remuneration system in the TS (Ripple (2017)).

5.2.2. Ethereum and Dapps

The TS is about providing distributed computing in a P2P network. This requires a mean for consumers to transfer rewards to providers in exchange for their service, which can be done by deploying smart contracts. Ethereum runs these smart contracts, in turn. Thus, the TS could implement the Ethereum-based technology for their reward system to enable direct payments between consumers and providers.

In Buterin (2014), it was already proposed that cloud computing could be based on Ethereum's EVM technology. Users could then ask their peers to carry out computations or they can offer spare CP to the network. This idea has existed since 2000, when Stanford researchers needed additional CP for their data analyses and founded the distributed computing project Folding@home (Front Page (2017)).

People could “donate” their idle CP of personal computers from their home and all over the world. With Ethereum, this process could finally be monetized and applied to other projects as well. By installing the technology, almost perfect competition would exist. Ethereum as an open-source platform gives providers and consumers access to perfect information. The CP is a homogenous trade good and all participants have a relatively small market share. Thus, no participant has the market power to set prices. Furthermore, entry and exit barriers are low, which can attract users to join the network and rent out their resources within the network. For this reason, computation costs can be lowered. TS could define price setting conditions and restrictions, or specify the pairing of consumer with provider through smart contracts. Thus, an efficient allocation of business partners based on their preferences and budget could be made. For instance, one user is indifferent about the price, but wants the computation to be as fast as possible. This enables a market for distributed computing, in which anyone could participate with their device and receive a payment automatically after delivering the service.

This opportunity was already recognized by other developers. Two Dapps exist with similar concepts regarding cloud computing. The first one is Golem (Golem (2016a)), a decentralized sharing economy of CP. Similar to TS, it connects different devices in a P2P network and enables requestors to rent spare CP of providers. Special is, that these resources can be used to execute tasks requiring any amount of computation time and capacity, from research to machine learning. Golem not only provides a transaction system, it also enables developers to create and distribute software on an app-store-like function, and use the Transaction Framework to choose whatever remuneration model they desire in order to make a profit (or not) from their software (Golem (2016b), Golem (2016a)). Another Dapp, iEx.ec (iEx.ec (2017)), offers Ethereum blockchain-based distributed cloud computing as well. It works similar to Golem, but differs in some ways. Whereas Golem aims at creating a virtual supercomputer to attract users of High-Performance Computing, iEx.ec initially focuses on supporting Dapps to create a virtual cloud infrastructure (iEx.ec (2016)).

As clearly indicated above, the most appropriate remuneration system for TS would be based on the Ethereum blockchain due to its many benefits. TS would profit from its interoperability of different devices and secure transaction when exchanging value between peers. But above all, Ethereum decentralizes the market for distributed computing, thus giving fair and complete access to everyone. Thus, Ethereum provides the best solution for an individualized payment system in the TS.

6. Conclusion and Outlook

This chapter forms the content-related completion of the thesis. The paper will be closed with a conclusion and outlook for future development and research.

6.1. Conclusion

This work studied the current state of cryptocurrencies with emphasis on the prominent Bitcoin. Thereby, its related concepts and underlying technology were outlined. Bitcoin enables a decentralized network where no trusted authority controls transactions and data. However, the currency struggles with technical challenges and limitations. Various approaches to solve these issues through alternative currencies were proposed. Drawing from dispersed knowledge resources, Ethereum was identified to be the most promising to improve Bitcoin. Ethereum does not only serve as a digital currency, but also provides a decentralized platform, enabling the creation of smart contracts with applications in numerous fields. The short display of these applications and its effects, fueled by the blockchain technology, has shown its potential to transform the internet, leading to the rise of the Web 3.0. Not only will the digital world be affected by this technology, but also many other aspects in life. Based on the model of the TS, it was demonstrated how smart contracts could be implemented in distributed computing systems to deploy an individualized remuneration system.

Due to the limitation of research time and the high number of different cryptocurrencies and their applications, the thesis merely focuses on the most influential ones and their alternative solution approaches. Since the topic of blockchain is relatively new and unexplored, except for its application on Bitcoin, only a fraction of its potential applications could be presented, including its implementation in the TS. For simplicity reasons, highly technical and mathematical content of the specific currencies, such as codes, are not closer examined.

6.2. Outlook

Although Bitcoin’s framework may be limited, it will still play an important role in the future due to its dominance in the cryptocurrency market. In order to retain its leading position, its limitations and vulnerabilities have to be addressed. As suggested by Yli-Huumo et al. (2016) more research has to be done, especially on scalability issues, to enable the pervasive use of blockchain technology.

With blockchain, intermediaries and centralized authorities for transactions are not needed anymore. However, its impact goes far beyond Bitcoin. Thus, research should not only focus on Bitcoin systems, but also explore blockchain’s potential for other applications. Its facilitation of smart contracts could reshape the digital world and how people will engage with each other. It allows for the automated execution of complex tasks, while being tamper-proof. This leads to lower costs and also trustless interaction of peers in fully decentralized autonomous organizations.

Even though the application of smart contracts in ecosystems like Ethereum is a novelty, it has shown a rapid development already and challenges existing systems and processes, leading to new business models and ubiquitous Dapps. Therefore, this field has to be further explored to pave the way for the Web 3.0.

References

Alliance, S. C. Smart contracts: 12 use cases for business and beyond. *Chamber of Digital Commerce*, page 56, 2016. Washington D.C.

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., and Virza, M. Zerocash: Decentralized anonymous payments from bitcoin. In *IEEE Symposium on Security and Privacy*, pages 459–474, San Jose, CA, 2014. IEEE.

Berke, A. How safe are blockchains? it depends. *Harvard Business Review*, 2017.

Biryukov, A., Khovratovich, D., and Pustogarov, I. Deanonymisation of clients in bitcoin p2p network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 15–29. ACM, 2014.

Blockchain.info. Blockchain size. URL https://blockchain.info/en/charts/blocks-size. retrieved 2017-05-11.

Blockchain.info. Gesamtzahl aller bitcoin-transaktionen weltweit bis märz 2017, 2017.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., and Felten, E. W. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *Security and Privacy (SP) (2015), No. 2015 IEEE Symposium*, pages 104–121. IEEE, 2015.

Bradbury, D. The problem with bitcoin. *Computer Fraud & Security*, 2013 (11):5–8, 2013.

Buterin, V. Ethereum: A next-generation smart contract and decentralized application platform. 2014.

Chaum, D. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, Springer US, 1983.

Christidis, K. and Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:12, 2016.

CoinMarketCap. Crypto-currency market capitalizations, 2017. URL https://coinmarketcap.com/all/views/all/. retrieved 2017-05-30.

Dahan, M. and Casey, M. Blockchain technology: Redefining trust for a global, digital economy, 2017. URL http://blogs.worldbank.org/ic4d/blockchain-technology-redefining-trust-global-digital-economy?cid=EXT_WBBlogSocialShare_D_EXT. retrieved 2017-05-17.

Ethereum. Ethereum project. URL https://www.ethereum.org/. retrieved 2017-05-16.

Eyal, I. and Sirer, E. G. Majority is not enough: Bitcoin mining is vulnerable. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 8437, pages 436–454. Springer, 2014.

Front Page. Folding@home, 2017. URL https://folding.stanford.edu/. retrieved 2017-05-21.

Gandal, N. and Halaburda, H. Competition in the cryptocurrency market. (14–17):33, 2014.

Golem. The golem project, 2016a. p. 28.

Golem. How and why golem will change the world (or at least the internet), 2016b. URL https://github.com/golemfactory/golem/wiki/FAQ.

IBM. Ibm knowledge center - public key cryptography, 2017a. URL https://www.ibm.com/support/knowledgecenter/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55940_.htm. retrieved 2017-04-27.

IBM. Ibm knowledge center - digital signatures, 2017b. URL https://www.ibm.com/support/knowledgecenter/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55190_.htm. retrieved 2017-04-27.

iEx.ec. A new cloud computing platform at the ethereum smart contracts bit.news, 2016. URL https://bit.news/eng/iex-ec-new-cloud-computing-platform-ethereum-smart-contracts/. retrieved 2017-05-22.

iEx.ec. Blockchain-based fully distributed cloud computing, 2017. URL http://iex.ec/. retrieved 2017-05-22.

Karame, G., Androulaki, E., and Capkun, S. Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin. *IACR Cryptology ePrint Archive*, 2012:1–17, 2012.

Lewis, A. A gentle introduction to ethereum. URL https://bitsonblocks.net/2016/10/02/a-gentle-introduction-to-ethereum/. retrieved 2017-05-16.

Litecoin. Open source p2p digital currency, 2017. URL https://litecoin.org/. retrieved 2017-05-09.

Marvin, R. Tech that's changing the world. *PC Magazine*, 2017.

Miers, I., Garman, C., Green, M., and Rubin, A. D. Zerocoin: Anonymous distributed e-cash from bitcoin. In *IEEE Symposium on Security and Privacy*, pages 397–411. IEEE, 2013.

Moreno-Sanchez, P., Zafar, M. B., and Kate, A. Listening to whispers of ripple: Linking wallets and deanonymizing transactions in the ripple network. *Proceedings on Privacy Enhancing Technologies*, 2016(4):436–453, 2016.

Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system, 2008. p. 9.

Nielsen, M. How the bitcoin protocol actually works — data-driven intelligence. URL http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/. retrieved 2017-04-14.

O'Dwyer, K. J. and Malone, D. Bitcoin mining and its energy footprint. *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014CIICT 2014)*, page 280–285, 2014.

Pagliery, J. Fbi shuts down online drug market silk road fbi busts black market bazaar silkroad, arrests its alleged mastermind. CNN Money, Oct. 2, 2013 2013. URL http://money.cnn.com/2013/10/02/technology/silk-road-shut-down/. retrieved 2017-05-01.

Perez, S. Spotify acquires blockchain startup mediachain to solve music's attribution problem. TechCrunch. URL https://techcrunch.com/2017/04/26/spotify-acquires-blockchain-startup-mediachain-to-solve-musics-attribution-problem/. retrieved 2017-05-17.

Reid, F. and Harrigan, M. An analysis of anonymity in the bitcoin system. In *Security and Privacy in Social Networks*, page 197–223, New York, 2013. IEEE, Springer.

Ripple. Technology, 2017. URL https://ripple.com/technology/. retrieved 2017-05-20.

Schäfer, D., Edinger, J., VanSyckel, S., Becker, C., and Paluska, J. M. Tasklets: "better than best-effort" computing. In *Proceedings of the "25th IEEE International Conference on Computer Communication and Networks (ICCCN 2016)"*, pages 1–11. IEEE, 2016a.

Schäfer, D., Edinger, J., VanSyckel, S., Paluska, J. M., and Becker, C. Tasklets: Overcoming heterogeneity in distributed computing systems. In *Proceedings - 2016 IEEE 36th International Conference on Distributed Computing Systems Workshops*, pages 156–161. IEEE, 2016b.

Schwartz, D., Youngs, N., and Britto, A. The ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*, pages 1–8, 2014.

Silva, J. E. An overview of cryptographic hash functions and their uses. *GIAC*, 2003.

Szabo, N. Smart contracts: Building blocks for digital markets. 1996.

Tasca, P. Digital currencies: Principles, trends, opportunities, and risks. *Deutsche Bundesbank and ECUREX Research*, page 110, 2015.

The Homestead Documentation Initiative. What is ethereum? — ethereum homestead 0.1 documentation. URL http://ethdocs.org/en/latest/introduction/what-is-ethereum.html. retrieved 2017- 05-14.

Tschorsch, F. and Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, 18(3):2084–2123, 2016.

Underwood, S. Blockchain beyond bitcoin. *Communications of the ACM*, 59 (11):15–17, 2016.

Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, page 32, 2014.

Xie, L. A beginner's guide to litecoin – the coinbase blog, 2017. URL https://blog.coinbase.com/a-beginners-guide-to-litecoin-d9b455d44cd3. retrieved 2017-05-27.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., and Smolander, K. Where is current research on blockchain technology?—a systematic review. *PloS one*, 11 (10), 2016.