UHASSELT

KNOWLEDGE IN ACTION

www.uhasselt.be
Universiteit Hasselt
Campus Hasselt:
Martelarenlaan 42 | 3500 Hasselt
Campus Diepenbeek:
Agoralaan Gebouw D | 3590 Diepenbeek

UHASSELT

KNOWLEDGE IN ACTION

Faculty of Business Economics

Master of Management

Master's thesis

Technical comparison between blockchain and Holochain

Martijn Rubbrecht

Thesis presented in fulfillment of the requirements for the degree of Master of Management, specialization Business Process Management

SUPERVISOR :

Prof. dr. Benoit DEPAIRE

2019
2020

Faculty of Business Economics

Master of Management

Master's thesis

_Technical comparison between blockchain and Holochain

Martijn Rubbrecht

Thesis presented in fulfillment of the requirements for the degree of Master of Management, specialization Business Process Management

SUPERVISOR :

Prof. dr. Benoit DEPAIRE

Technical comparison between blockchain and Holochain[1]

Martijn Rubbrecht

Abstract *Since the creation of the Bitcoin blockchain in 2008, multiple developers have created numerous Bitcoin blockchain alternatives, such as Ethereum, Ripple and Bitcoin Cash. However, all suffer from three issues that are pervasive throughout all blockchains: scalability, data privacy and interoperability. In 2018, ten years after the publishing of the Bitcoin whitepaper, a new whitepaper was released in order to introduce the world to a new technology: Holochain. Holochain thinks "outside the blocks" by shifting from a data-centric structure to an agent-centric structure as to mimic how nature organizes itself. Holochain promises scalable, distributed applications with data integrity that offer versatile solutions. This paper introduces the technology and qualitatively compares it to the Bitcoin blockchain in terms of scalability, data privacy and interoperability. The findings are that Holochain offers improvement in all three categories. Holochain applications scale linearly with computational power on the network, while the Bitcoin blockchain is unaltered if new users enter the network. Holochain also allows developers to configure their applications to their needs, in order to build a rich ecosystem of narrow-focused Holochain applications that work together. Bitcoin, on the other hand, is a monolithic network. Last, data privacy in Holochain is slightly improved by using a validating DHT instead of copying all data to all nodes, as is the case with Bitcoin. However, both technologies suffer from similar security issues related to dual-key cryptography. The research is based on existing academic literature and web documents.*

Index terms *Blockchain, Bitcoin, Holochain, scalability, interoperability, privacy*

1 INTRODUCTION

In 2008, Satoshi Nakamoto released the white paper "Bitcoin: A Peer-to-Peer Electronic Cash system" which brought Bitcoin and the underlying technology, blockchain, to life (Nakamoto, 2008). The technology is a response to the financial uncertainty and crisis effects, and proposes an alternative to the central banks' functions in a time of mistrust of handling the recession period (Sas & Khairuddin, 2015). A few months after the introduction of the technology, the Bitcoin network became functional and is up to now (April 2020) still the most traded cryptocurrency in the world (Dumitrescu, 2017) [1].

Although Bitcoin was initially conceived as a financial transaction protocol, due to cryptographic security benefits of blockchain technology, such as pseudonymous identities, decentralization, fault tolerance, transaction integrity and authentication, it is dramatically expanding beyond the financial industry into other domains of society (Makhdoom et al., 2019) (Tang et al., 2019). Among others, Blockchain is finding its way in healthcare (McGhin et al., 2019) (P. Zhang et al., 2018), supply chain management (Longo et al., 2019) (Tönnissen & Teuteberg, 2020) (Wamba & Queiroz, 2020), smart cities (Sharma & Park, 2018) (Sun et al., 2016), the physical internet (Meyer et al., 2019) and the Internet of Things (IoT) (Makhdoom et al., 2019) (Reyna et al., 2018) (Y. Zhang & Wen, 2017).

Today, hundreds of virtual currencies are clones of the famous Bitcoin, differing by issuance scheme, block time or supply. They are all known under the name of altcoins (Dumitrescu, 2017). The most popular altcoins at the time of writing are Ethereum [ETH] (Buterin, 2013), Ripple [XRP] (Chase & MacBrough, 2018), Tether [USDT] (Pierce et al., 2016) and Bitcoin Cash [BCH] [2].

However, although multiple variations of Bitcoin are created, at least three key challenges are pervasive across all applications and have not yet been solved cleanly. These are data privacy, scalability and interoperability (Underwood, 2016). In addition, confirming transactions in the blockchain requires a significant amount of computational power (Yli-Huumo et al., 2016). According to an online tool released by the University of Cambridge,

[1] *This master thesis was written during the COVID-19 crisis in 2020. This global health crisis might have had an impact on the (writing) process, the research activities and the research results that are at the basis of this thesis.*

Bitcoin uses an estimated 76 terawatt-hours (TWh) of electricity per year, approximately 0.30% of the total global electricity consumption [3] [4]. These issues at least partially clarify why transformative applications are still not commercially available and why few organizations have progressed their blockchain solutions beyond the feasibility or prototype stage (Hughes et al., 2019).

As a solution, Arthur Brock, Eric Harris-Braun and Nicolas Luck proposed an agent-centric distributed computing platform called Holochain (Harris-Braun et al., 2018). As mentioned by Arthur Brock, Blockchain technology has a fundamental scalability problem due to the fact that "all of the nodes that are participating in it […] have to end up with one global ledger, which means essentially everybody has to do all of the work. It doesn't get more efficient as you add more nodes, it gets less efficient" [5]. The authors of the whitepaper try to tackle this scalability problem by shifting from a data-centric approach to an agent-centric approach.

Although this agent-centric approach is promising, barely any academic literature is found on Holochain. This paper therefore aims to provide an initial overview and understanding of this emerging technology. In addition, it intends to clarify if the above-mentioned pervasive issues throughout Blockchain technology are resolved.

The paper is ordered as follows. Section 2 points out the research gap, expresses the problem statement and the corresponding research questions, and elaborates on the research methodology used to structure the analysis. Section 3 and 4 describe the working principles, characteristics and limitations of the Bitcoin blockchain and Holochain respectively. Section 5 compares the two technologies in terms of scalability, data privacy and interoperability. Section 6 concludes the findings and section 7 gives directions for future research and presents the limitations of this analysis.

2 PROBLEM STATEMENT

2.1 RESEARCH GAP

Ever since the Bitcoin whitepaper has been published, Bitcoin and the underlying blockchain technology have risen in popularity. Blockchain technology is often included in listings of key technology trends, which are "trends that are shifting, changing, reaching key tipping points and/or are driving disruption" [6]. Among others, it has been included in the listings of Gartner (*Gartner Top 10 Strategic Technology Trends for 2020*) [7], Forbes (*Top Tech Trends To Watch In 2020*) [8] and Deloitte (*Tech Trends 2020*) [9]. It is clear that blockchain technology has the potential to significantly transform many industries. However, while interest is high, the majority of blockchain implementations are still in alpha or beta stages due to significant technological challenges (Woodside & Jr, 2017). Three of these technological challenges are scalability, data privacy and interoperability (Underwood, 2016).

Holochain has been developed to resolve issues related to blockchain technology by shifting from a data-centric approach to an agent-centric approach. In fact, Holochain stems from the MetaCurrency project which has roots even before the launch of Bitcoin [10] [11]. As of now, the technology has up and running applications, such as Clutter (a peer-to-peer version of Twitter), Junto (a peer-to-peer social media platform) [12] and RedGrid (a software protocol that can be integrated into devices that produce, consume, or store electricity to create The Internet of Energy, abbreviated as IoE) [13]. In addition, the technology is supported by multiple persons, one of them being Jim Cook, co-founder of Netflix and Mozilla [14].

In other words, Holochain is a promising technology and, in addition, is delivering on promises. However, when performing a search "Holochain" on the UHasselt university library or HBR, no academic articles are returned. A search on Google Scholar returns a handful of articles, but these only mention Holochain. To clear this research gap, this paper aims to give an initial introduction to Holochain as well as verify if the three issues related to Blockchain are resolved.

2.2 RESEARCH QUESTIONS

The following research questions help to structure the approach and to reach a final verdict about the technology.

(1) What is Holochain?
(2) What are the differences between Holochain and Bitcoin?
(3) Does Holochain offer an improvement over Bitcoin towards the issues of scalability, data privacy and interoperability?

Due to time restrictions, only one blockchain protocol can be compared to Holochain. The Bitcoin protocol is chosen because of two main reasons. First, Bitcoin is the first application of the blockchain technology and is still the most popular among all blockchain protocols. Second, because of this popularity, enough academic literature can be found on Bitcoin.

2.3 RESEARCH METHODOLOGY

A qualitative research approach is chosen due to several reasons. First and foremost, there is a clear lack of academic literature on Holochain which results in a study of exploratory nature. A qualitative research approach is preferred in this scenario, as recommended by Goethals (Goethals et al., 2004). Second, Holochain, just as Blockchain, is a complex technology for which an in-depth analysis is favored. Third, scalability, interoperability and data privacy are all context dependent. A qualitative research approach takes this context into consideration, as opposed to a quantitative one.

Some of the commonly used qualitative research methods are interviews, surveys, focus groups, case studies and a literature review (Ahmed et al., 2016) [15]. A literature review is chosen due to the following reasons. First, this paper aims to provide an initial introduction to Holochain, not an in-depth investigation. Second, due to the novelty of the technology, there is a lack of academic content on and case studies about the technology. This also forces the study to use inductive logic in order to build theory. Furthermore, a (post-)positivist paradigm is selected as a result to the exploratory nature of the study (Goethals et al., 2004). Table 1 summarizes the research design choices used in this paper.

Table 1: Overview of the research design choices.

Research characteristic	Design choice
Type	Exploratory study
Nature	Qualitative research
Method	Literature review
Paradigm	(Post-)positivist
Logic	Inductive

3 BITCOIN

As mentioned in the introduction, the Bitcoin whitepaper, written by the anonymous author(s) Satoshi Nakamoto, has been released on 31 October 2008 (Nakamoto, 2008). Nakamoto claimed there was a need for a purely peer-to-peer version of electronic cash that would bypass the financial institutions. Although Bitcoin was not the first attempt of an electronic cash system (for example, E-Gold and E-cash were launched before) [16], it was the first to solve the double-spending problem [17]. The official launch of Bitcoin happened three months after the publishing of the whitepaper, on 3 January 2009 (Dumitrescu, 2017).

Bitcoin manages the double-spending problem by implementing a confirmation mechanism and maintaining a universal ledger, called blockchain [17]. In essence, a blockchain is a series of 'blocks', chained together with complex computational algorithms. These blocks contain data of transactions (Woodside & Jr, 2017).

3.1 COMPONENTS

This section elaborates on the essential components of the Bitcoin blockchain. These are the distributed ledger, the confirmation mechanism and the transactions.

3.1.1 The distributed ledger

The distributed ledger is a sequence of blocks, in which each block contains a collection of transactions. The sequence of the blocks is fixed by making use of cryptography, namely hashing.

3.1.1.1 <u>Block</u>

A block consists of five elements: a "magic" number, the block size, the transactions, the transaction counter and the block header [18]. The "magic" number is an arbitrary number of four bytes[2] which is used in programming to signal the type of software, so the software can identify itself. This magic number is the same for all Bitcoin blocks. The block size shows the size of the block and has a length of four bytes. Note that the block size of a Bitcoin block is limited to a maximum size of 4 MB [19], however, the average block size is roughly 1 MB [20]. Next, the block contains a list of all transactions that are stored in this particular block. The transaction counter, which is an integer with a length between one and nine bytes, simply displays the number of transactions stored in the block. The amount of transactions that can be stored in a block is dependent on the size of the block and the size of the transactions itself [21]. However, the average Bitcoin block contains roughly 500 transactions [22]. Last, the block header is a number of 80 bytes and is one of the most important constructs of the blockchain [23] [18]. However, before explaining the block header, the concept of hashing is explained.

3.1.1.2 <u>Hashing</u>

A hash is a function that converts an input of letters and number into an encrypted output of a fixed length. This increases security since anyone trying to decrypt the hash won't be able to tell how long or short the input is simply by looking at the length of the output [24].

[2] One byte is a collection of 8 bits. A bit has two states, 0 or 1.

One of the most used hashing algorithms, also used by Bitcoin, is SHA 256. SHA stands for "secure hash algorithm". When hashing "Bitcoin" for example, the result is the following [25]:

b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4

Note that the result of the hashing algorithm is a number in the hexadecimal number system. For more information about the number systems, see appendix A.

A hashing algorithm has several important characteristics (Naor & Yung, 1989; Schepers, 2018):

(1) The function is deterministic, meaning the same input always results in the same output.
(2) The function is easy to compute.
(3) A small change in the input results in a large change in the output. This is called the "avalanche effect" [26].
(4) The function is a one-way function, meaning it is infeasible to invert the function (pre-image resistance).
(5) Given an input x, it is difficult to find an input y, satisfying $h(x) = h(y)$ and $x \neq y$ (second pre-image resistance).
(6) It is difficult to find two strings x and y, with $x \neq y$, satisfying $h(x) = h(y)$ (collision resistance).

3.1.1.3 Block header

The block header of a Bitcoin block contains six elements: the version, the hash of the previous block, the time, a nonce ("number used once"), the bits target and the hash Merkle root. The version is a four-byte number which indicates the version of the Bitcoin protocol used. In other words, this number indicates which set of blockchain rules to follow, as these rules can change slightly over time. The hash of the previous block is a 32-byte (or 256 bits) long hash. It is this feature that links all blocks together in a specific order, thus creating a "chain of blocks". Next, the block is timestamped by adding a four-byte number which denotes the time. This time stamping is just one convenient way of ordering transactions in consensus systems [27]. In addition, it allows you to later certify that the document or data existed at that time and publicly prove that you have certain information without revealing the data or yourself [28]. This also works the other way around, only if the transaction exists at that point in time can the corresponding hash value be obtained [29]. Next, the nonce and bits target are both numbers of four bytes and are essential for the mining process, which will be explained later. The last element of a block header is the hash of the Merkle root, which is, again, a number with a length of 32 bytes. This number contains information from all the transactions stored in that particular blockchain and will be explained in the next section [23] [18]. Note that the total amount of bytes in a block header, which is simply the sum of its elements, equals to 80, as mentioned earlier.

3.1.1.4 Merkle tree

A Merkle tree is a data structure that is used to encode blockchain data more efficiently and securely. Instead of combining all transactions, hashing the result and using this hash to insert the transactions in the block header, a tree of hashes if formed, as depicted by Figure 1. As shown, each transaction is hashed, then each pair of transactions is concatenated and hashed together, and so on until there is one hash for the entire block. This "top-level" hash is called the Merkle root and this hash is stored in the block header. Note that if one transaction in the Merkle tree is changed, even by a bit, the hash of that transaction would differ largely due to the avalanche effect. This change will then propagate its way to the top of the Merkle tree and finally alter the hash of the Merkle root, which is saved in the block header. This is one of the features that gives blockchain technology its immutability characteristic, as will be explained later. Notice that that the structure of the Merkle tree in fact resembles a tree, explaining the name.

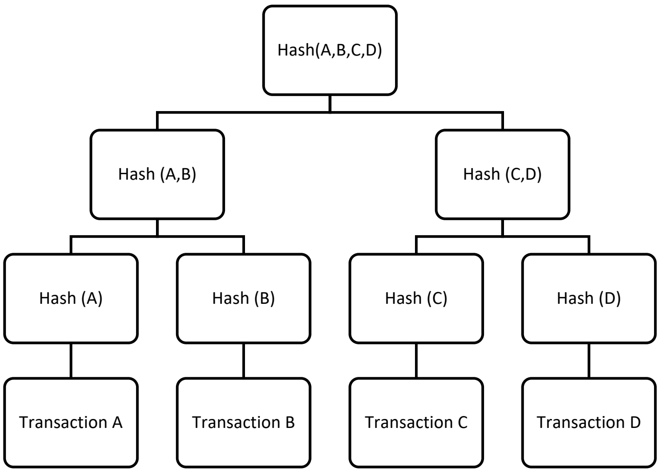

Figure 1: An example of a Merkle tree with four transactions.

Also note that an average Bitcoin block contains 500 transactions, making the structure larger than depicted in the example, which uses only four transactions [22].

3.1.1.5 Intermediate summary

At this moment, a chain of blocks can be formed since each block is linked to the previous one by adding the hash of the previous block into the current block header, as depicted in Figure 2. This chain of blocks is immutable since a change in any content of an existing block would result in a change of the hash of the block, which would cause the hash of the next block to be different and so on. As a result, a whole new chain of blocks would be formed.

Due to this structure, all content stored on a particular chain of blocks, including the transactions stored in a block, are safe from tampering.

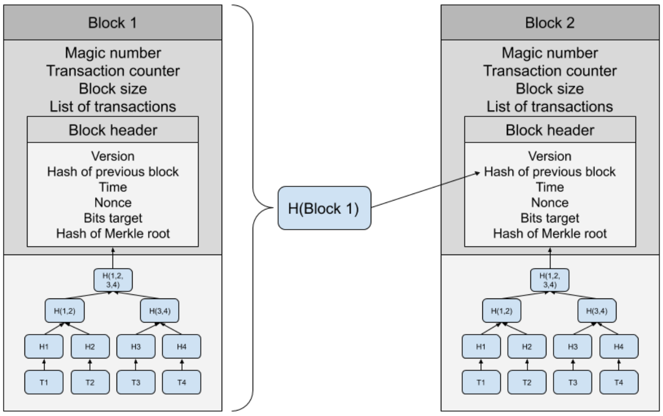

Figure 2: Chaining of blocks.

3.1.2 Confirmation mechanism

As shown above, if a piece of information stored in a block would be altered, a new chain will be formed. Since Bitcoin distributes only one universal ledger to all its participants, a confirmation mechanism is required so that all participants can agree on a single universal ledger.

The most common confirmation mechanism, also used by Bitcoin, is the Proof-of-Work concept, which will be explained in the next section [30].

3.1.2.1 Proof-of-Work (PoW)

The Proof-of-Work (PoW) idea was first published in 1993 and the term first used in 1999. However, the mechanism went largely unnoticed until Satoshi Nakamoto applied the technique to Bitcoin in 2008 [31] [32]. The basic idea of the Proof-of-Work mechanism is to elect one leader that decides the contents of the next block. This leader is also responsible for broadcasting the block to the network, so that the other peers can verify the validity of its contents [30]. In order to be elected as the leader for the next block, a mathematical puzzle needs to be solved. This puzzle is the following:

> *Given data X, find a number n such that the hash of n appended to X results is a number less than Y* [30].

The given data X is the content of the block [33], of which the components are described in the previous section. The number Y is implied by the bits target. Note that both X and Y are fixed and stored in the block. The number n is a nonce (a "number used once") and is variable. All participants on the Bitcoin network trying to solve this mathematical puzzle are called miners. The first miner to find a nonce that in combination with the data X creates a hash that starts with a number of zeros equal to or greater than the bits target, wins the race. He or she adds the nonce to the block header and broadcasts the block to the network. Other miners can then verify the validity of the solution by running the hash algorithm with the contents of the block (X) and the nonce, and checking if the resulting hash is less than the number Y. Or in other words, checking if the resulting hash starts with a number of zeros that is greater than or equal to the bits target [33] [34] [35] [36] [28]. This verifying is easy and only takes a few seconds due to the second property of hash functions, that is, the hash function should be easy to compute.

Note that the difficulty of the puzzle can be increased by increasing the bits target, which results in a lower value of the number Y. On the Bitcoin protocol, the difficulty level is set in such a way that one block is approximately mined every 10 minutes. This difficulty level is adjusted every 2016 blocks, which takes around two weeks (Buterin, 2013) [37]. The difficulty of the Proof-of-Work mechanism on the Bitcoin protocol is thus dependent on the computing power of the network.

3.1.2.2 Collision

It is a possibility that two miners solve the mathematical puzzle at the same time, thus, for a brief moment, generating two blockchains. Nodes will consider the first block they receive as part of their blockchain, but also keep the second block they receive just in case. However, the second block to arrive will not be considered as part of their active blockchain. Consequently, nodes on the network will be in disagreement about which of these two blocks belong at the top of the chain. The disagreement is resolved when the next block is mined, since this block will be placed on top of one of these blocks, creating a new longest chain of blocks [38]. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it (Nakamoto, 2008).

Because of this issue, it is usually recommended to wait for a few (most articles mention six) confirmed blocks on top of the block containing your particular transaction in order to consider your transaction as probabilistically final [39].

3.1.2.3 Mining incentive

The objective of the Proof-of-Work mechanism is to be the first to solve the mathematical puzzle. This allows the winning miner to "be the leader" and decide which contents to be added to the Bitcoin blockchain. However, most importantly for the miners is that Bitcoins are earned when a block is mined successfully. This happens in two ways.

First, for every new block that is mined, a fixed number of Bitcoins are released, and these are attributed to the winning miner. In other words, miners are basically "minting" currency, explaining the name "mining" [40]. The current Bitcoin block subsidy is 12.5 bitcoins per block, which amounts to, at the time of writing[3], almost €90 000! This subsidy per block, however, halves every 210 000 blocks [41]. There is a limit to halving Bitcoins, however. The smallest unit available in Bitcoins is the Satoshi, which represents one hundred millionths (10^{-8}) of a Bitcoin [42]. Due to the fact that the subsidy is halved every 210 000 blocks and the limit to the division of Bitcoins, the total amount of Bitcoins to be mined is capped at 21 million. As a result, there will come a time when bitcoin mining ends. However, this ending is not expected until 2140 [40].

The second way miners can earn Bitcoins, and the only one after all Bitcoins are mined, is by collecting transaction fees. Bitcoin blocks have a theoretical maximum size of 4 MB which limits the number of transactions that can be stored in a block. Since miners are looking to maximize their profits, they will prioritize the transactions with the highest fees. Users can add a fee to their transaction so that a miner is stimulated to insert that particular transaction into the block he/she is about to solve a mathematical puzzle for. Although these fees are optional for a user, as a practical matter, a transaction without one might have to wait a long time to be processed if the network is congested. The transactions fees are expected to become a more important source of remuneration for miners as the block reward falls [43].

3.1.2.4 Types of nodes

There are different types of nodes on the network depending upon their capabilities and resources such as computation capability and memory size (Makhdoom et al., 2019). The Bitcoin network has four types of nodes: light nodes, full nodes, super nodes and mining nodes [44]. Note that these nodes take on different roles on the network but are all equal due to the peer-to-peer, decentralized characteristic of the Bitcoin network [45].

- Light nodes can only send and receive transactions and do not store the complete copy of the blockchain.
- Full nodes validate transactions and blocks and maintain a complete copy of the blockchain. They do not mine blocks, however. They accept transactions and blocks from other full nodes, validate these based upon the consensus rules of the respective blockchain and then relay them further to other full nodes. Most full nodes also serve light nodes by allowing them to transmit their transactions to the network and by notifying them when a transaction affects their wallet [46]. Note that full nodes are essential for the security of the blockchain, since these make the network decentralized (Makhdoom et al., 2019).
- Super nodes are full nodes which generally operate around the clock to help connect other full nodes to each other and spread the blockchain across the entire network [44].
- Mining nodes are full nodes and have the additional capability to mine or validate new blocks, thus extending the blockchain.

3.1.3 Transactions

In the previous sections, the distributed ledger and the confirmation mechanism have been described. This section briefly explains how transactions are added to the blocks and how they can be linked to individuals, which explains how individuals are not anonymous on the blockchain, but rather pseudonymous.

3.1.3.1 Transactions

A transaction is a data structure that encodes a transfer of value from a source of funds, called an input, to a destination, called an output. A transaction contains the following fields: the version, the locktime, the transaction inputs, the input counter, the transaction outputs and the output counter [18] (Antonopoulos, 2017). The version is a four-byte number which indicates the version of the Bitcoin protocol used, as discussed before. The locktime is an integer with a length of four bytes that defines the earliest time that a transaction can be added to the blockchain. Most of the time, it is set to zero. The input and output counters display the number of transaction inputs and transaction outputs respectively. They are integers with a length between one and nine bytes, just as the transaction counter in the block. The transaction inputs are unspent transaction outputs (UTXO) consumed by the transaction, while transaction outputs are unspent transaction outputs (UTXO) created by the transaction. The average transaction size is roughly 600 bytes [47].

3.1.3.2 Unspent transaction outputs (UTXO)

Unspent transaction outputs are the fundamental building blocks of a Bitcoin transaction. UTXO are indivisible chunks of Bitcoin currency locked to a specific owner. As a result, an individual never has a "balance" of Bitcoins,

[3] Tuesday 28th of April 2020.

there are only UTXO locked to specific owners. An owner, however, can summon the number of UTXO linked to him/her by using a wallet, which scans the blockchain and aggregates all UTXO belonging to that user (Antonopoulos, 2017).

However, a user does not operate under his real name on the Bitcoin blockchain, but rather under a pair of cryptographic keys: a public and a private key. The two keys are related, in fact, the public key is generated from the private key, but it is impossible to derive the private key from the public key. The public key is publicly visible and is the address other users can send Bitcoins to. The private key, however, is highly personal and it is essential it is kept secret and safe [48]. The private key is used to sign UTXO so they can be linked to others [49].

Note that when a transaction request is submitted, the protocol checks all previous transactions to confirm that the sender has the necessary bitcoin as well as the authority to send them [48].

3.2 CHARACTERISTICS OF BITCOIN

This section covers some of the most prominent benefits and limitations of the Bitcoin blockchain.

3.2.1 Benefits

Dresher (Kube, 2018) identified the following key characteristics of blockchain: immutability, append only and time stamped, secure, and open and transparent. The key characteristics are briefly described below.

3.2.1.1 Immutability

Once a transaction is added to the blockchain, it cannot be altered. This statement is true as long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, since they will generate the longest chain and outpace attackers (Nakamoto, 2008).

3.2.1.2 Append only and time stamped

All records are date and time stamped, thereby ensuring a built-in audit trail is maintained for all additions to the network. In fact, the timestamp server has to verify that the timestamp of the block is greater than the timestamp of the previous block in the chain and less than two hours into the future (Vujicic et al., 2018). Due to the timestamping, data can only be added to the blockchain in time-ordered sequential order.

3.2.1.3 Secure

All additions to the blockchain are governed via secure algorithms that use public key encryption, thereby reducing the risk of data corruption or fraud (Hughes et al., 2019).

3.2.1.4 Open and transparent

The Bitcoin blockchain is a public, distributed ledger, meaning that all nodes in the network share the same universal ledger. Furthermore, this universal ledger, including the public keys, are all publicly visible. These characteristics make the blockchain more accurate and consistent across the entire network (Hughes et al., 2019).

3.2.2 Limitations

Although Bitcoin offers multiple advantages, a few technical challenges and limitations have been identified. These are throughput, size and bandwidth, latency, security, wasted resources, privacy and versioning (Yli-Huumo et al., 2016). These limitations will be briefly discussed.

3.2.2.1 Throughput

Blocks on the Bitcoin network have a theoretical block size limit of 4 MB. However, the average block size amounts to roughly 1 MB [50]. This results in a throughput of less than 7 transactions per second. In comparison, the payment network VISA achieved 47 000 transactions per second during the 2013 holidays. If the Bitcoin network were to copy this volume with an average block size of 1 MB and an average transaction size of 300 bytes, it would require a throughput of 8 GB per block, which would lead to over 400 TB of data per year (Vujicic et al., 2018)! This brings us to the next issue of the Bitcoin network, size and bandwidth.

3.2.2.2 Size and bandwidth

At the moment, the size of the bitcoin network is over 250 GB [51]. Remember that all full nodes store the complete history of the Bitcoin blockchain in order to validate all transactions all the way to the first block. The security of the Bitcoin network, in other words, can be gauged by the number of full nodes [52]. However, as the Bitcoin blockchain grows in size, the full nodes have to adapt their hardware in order to store this information. In addition, if the block size is increased as to increase the throughput, bandwidth becomes of importance as well. For example, if it takes 11 minutes for a full node to receive and validate a block, that node is no longer part of the Bitcoin blockchain, since a block is mined every 10 minutes. In other words, increasing the block size leads to fewer participants, centralizing and weakening the security of the Bitcoin network [53].

3.2.2.3 Latency

The processing time for a transaction in the Bitcoin network takes roughly 10 minutes. This processing time has been chosen on purpose to avoid chain splits and to create sufficient security. It will not be reduced in the future. Furthermore, as mentioned before, in order to increase security, it is recommended to wait for several confirmed transactions (usually six), which further increases latency (Treiblmaier, 2019). However, making a block and confirming the transaction should happen in seconds, while maintaining security. For example, it takes only a few seconds to complete a transaction in VISA, which is a huge advantage compared to blockchain (Yli-Huumo et al., 2016).

3.2.2.4 Security

Although blockchains offer a high security due to the distributed nature, there are still some types of attacks blockchains are susceptible to. The most well-known attack is the 51% attack (Reyna et al., 2018), in which an attacker node controls more computational power than the good nodes. This single entity would then have full control of the blockchain (Yli-Huumo et al., 2016). This attacker miner can defraud other users by sending them payments and then creating an alternative version of the blockchain in which the payments never happened. This new version is called a fork, as depicted on Figure 3. The attacker, who controls most of the mining power, can make the fork the authoritative version of the chain, since he/she can outpace the remaining network in terms of speed of adding blocks to the blockchain, therefore creating a new longest chain, and proceed to spend the same cryptocurrency again [54].

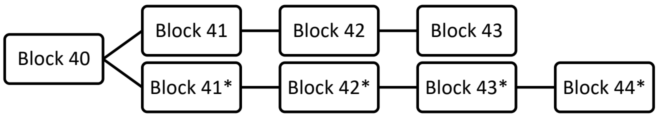

Figure 3: Forks on a blockchain.

Some other possible attacks are a distributed denial of service (DDoS) attack, race attack, Finney attack, Man in the Middle attack and Sybil attack (Reyna et al., 2018).

3.2.2.5 Wasted resources

Because of the high value of Bitcoins, more and more participants joined the network in order to earn Bitcoins, and thus real money. This has led to an increase of the computing power on the Bitcoin network, as depicted on Figure 4. At this moment, the computing power on the Bitcoin network is greater than 100 Exa hashes per second (EH/s) [55], which means the network is able to guess more than 100 000 000 000 000 000 000 nonces per second [56]. However, since the rate of blocks added to the Bitcoin network is fixed to one block every 10 minutes, the difficulty of the mathematical puzzle has increased accordingly. This leads to an improvement in security, since the odds of a 51% attack are less likely.

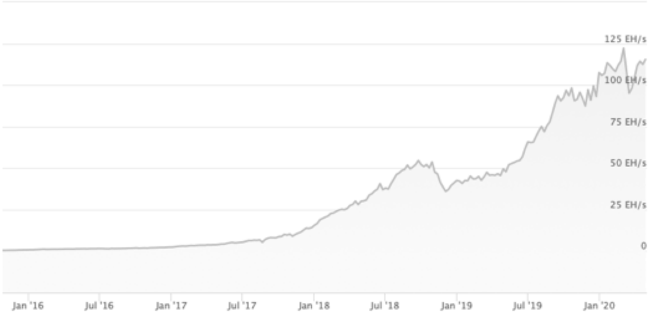

Figure 4: Bitcoin hash rate chart [57].

In order to improve a participant's odds of solving the mathematical puzzle, better performing hardware has been developed throughout the years. Currently, mining happens on expensive specialized hardware called Application Specific Integrated Circuits or ASIC chips [58]. These chips are developed to solely mine Bitcoins, and nothing else. An example of such an ASIC chip is the Innosilicon A10 Pro, which has a maximum hash rate of 500MH/s, a power consumption of 750W and a price tag over €3 000 [59]. Multiple people saw an opportunity in a steady income by investing in this hardware to form mining farms, which are entire plants and hangars full of these chips, outcompeting individual miners with discrete hardware. However, as an answer to these mining farms, individual miners started joining mining pools, which are collection of groups of miners working together to increase their chances of finding a block at the group level, compared to that at the individual level [60]. Bitcoin miners then pool their rewards equally between pool participants based on the number of shares they contributed to mining a block [61].

However, these evolutions (specialized hardware, mining farms and mining pools) have led to a centralization of the network, which increases the odds of a 51% attack, thus weakening the security of the Bitcoin network. In fact, in 2014, the mining pool "GHash.io4" temporarily reached 51% of the Bitcoin mining power (Reyna et al., 2018) [62].

3.2.2.6 Privacy

The Bitcoin blockchain is an open, distributed ledger, which means all of its contents are publicly visible. However, users do not operate under their real name on the Bitcoin blockchain but under a pair of cryptographic keys, made possible by a wallet. The public key is visible to the public, the private key is not. A user's privacy is preserved as long as the public key cannot be linked to his/her identity. However, as soon as somebody makes this link, the entire writing purchase history of this user becomes public [63].

3.2.2.7 Versioning

Code updates and optimization in blockchain networks are usually supported by part of the cryptocurrency community and are intended to improve their underlying protocols. These improvements are known as forks in the blockchain terminology (Reyna et al., 2018). The forks can be hard or soft, depending upon acceptance and removal by the upgraded (following new consensus rules) and non-upgraded nodes (following old consensus rules) (Makhdoom et al., 2019). However, as these forks create new chains of blocks, they become more susceptible to 51% attacks since a part of the nodes, and thus computing power, is lost.

An example of a hard fork is the creation of Bitcoin Cash (BCH), which happened in August 2017. BCH has, among others, implemented an increased block size of 8 MB to accelerate the verification process [64]. As illustrated by this example, a hard fork brings a radical change to the protocol, with no compatibility with previous blocks and transactions. Consequently, all the nodes have to upgrade to the latest update and nodes with older versions will no longer be accepted (Reyna et al., 2018).

3.3 OTHER BLOCKCHAINS

Due to the issues related to the Bitcoin network, several forks have happened, altering the network protocol while still remaining most of the working structure of Bitcoin. Some examples are Bitcoin Cash (BCH), Bitcoin XT and Bitcoin Classic [65]. However, other blockchains, with more drastic differences compared to Bitcoin, have been created as well. Some examples are Ethereum, Hyperledger and Ripple [66]. Some of the most common alterations are the following:

- Restricting the number of nodes that can process transactions, creating permissioned and permissionless blockchains.
- Restricting the number of participants on the network, creating private and public blockchains.
- Changing the consensus model.

3.3.1 Permissioned/permissionless blockchains

In a permissionless blockchain, any node can create new blocks of transactions, whereas in a permissioned blockchain, transactions processing is performed by selected nodes only (Makhdoom et al., 2019). The Bitcoin blockchain is a permissionless blockchain since every node can create new blocks of transactions.

3.3.2 Public/private/hybrid blockchains

Public, private and hybrid blockchains relate to the access to the blockchain data. Bitcoin is an example of a public blockchain in which anyone is allowed to join. Public blockchains are usually permissionless, however, permissioned, public blockchains do exist. In private blockchains, every participating node is selected and vetted. This increases privacy, which is one of the issues of a public blockchain [67]. Hybrid blockchains are, as the name suggest, a merge of private and public blockchain characteristics.

3.3.3 Consensus models

The most common consensus model is the Proof-of-Work model. However, other consensus models exist, such as the Proof-of-Stake (PoS) model, the practical Byzantine fault tolerance (PBFT) algorithm, the Proof-of-Activity, Proof-of-Authority (PoA) and many more. The PoS and PBFT models are briefly discussed below.

In the Proof-of-Stake (PoS) consensus model, the reward is given to the miners not based on their computations, as in the Proof-of-Work model, but on their coin holdings (Vujicic et al., 2018), as it is believed that participants with a great value share of the network are less likely to attack it (Meyer et al., 2019).

Another consensus model is the practical Byzantine fault tolerance (PBFT) algorithm. This consensus model is more efficient than PoW concerning latency and energy costs, but is less secure, as it can only tolerate up to 33% malicious nodes, as to 51% on the PoW model (Makhdoom et al., 2019). In the PBFT model, one miner determines the next block, which is added after two-thirds of the miners voted for it. Using PBFT, all miners should be known to the network, therefore this method can only be used in permissioned blockchains (Meyer et al., 2019). In addition, note that consensus methods that centralize the consensus among a limited number of users are more susceptible to a 51% attack (Reyna et al., 2018).

4 HOLOCHAIN

On 18 February 2018, Arthur Brock, Nicolas Luck and Eric Harris-Braun published the whitepaper of Holochain (Harris-Braun et al., 2018). The big difference between Holochain and blockchain is the shift from a data-centric structure to an agent-centric structure. This means that no true global consensus is maintained and, as a consequence, there is no energy-consuming consensus mechanism either. Instead, each agent on Holochain maintains a local, immutable chain. Parts of this local chain are stored in a validating, distributed hash table (DHT) [68]. The particular application the user wishes to use on the Holochain platform prescribes the set of ground rules on how to interact with and operate on the system. This set of rules is called the "DNA" of the app and, as will be explained later, also describes how often parts of the local chain are stored in the DHT.

4.1 COMPONENTS

As mentioned above, Holochain consists of three core components; the local source hash chain, the application and the shared storage in the form of a distributed hash table, abbreviated as DHT [69]. These three components are shown in Figure 5 and will be explained in the next sections.

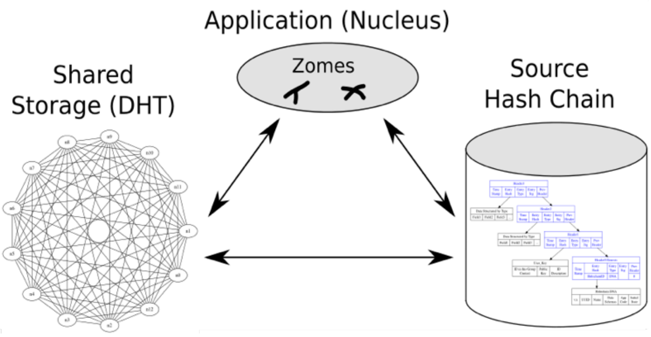

Figure 5: The components of Holochain [69].

4.1.1 Local source chain

Holochain does not maintain one single global ledger. Instead, every user of a Holochain application keeps a digital record of their actions and entries by writing to their local hash chain, one per application. This local hash chain implements several techniques from Blockchain in order to prevent people from tampering with their chain. First, as depicted on Figure 6, every entry or "block" on the local hash chain in Holochain is timestamped. This allows the creation of a logical sequence of entries. Second, the hash of the previous block is inserted into the new block, as to guarantee an immutable, append-only chain. Last, public key cryptography (a private and public key) is used to sign entries on this local chain [70]. Interactions involving multiple parties, such as a currency transfer between two people, are signed by each party and committed to both of their local chains [69]. This combination of existing techniques creates a tamper-proof local chain to which a user can only add data, but not alter already existing entries.

However, although users cannot alter previous entries on their local hash chain, they could delete their last entries and act like that particular transaction or action never happened in the first place. This is where the second component, the distributed hash table (DHT), comes into play.

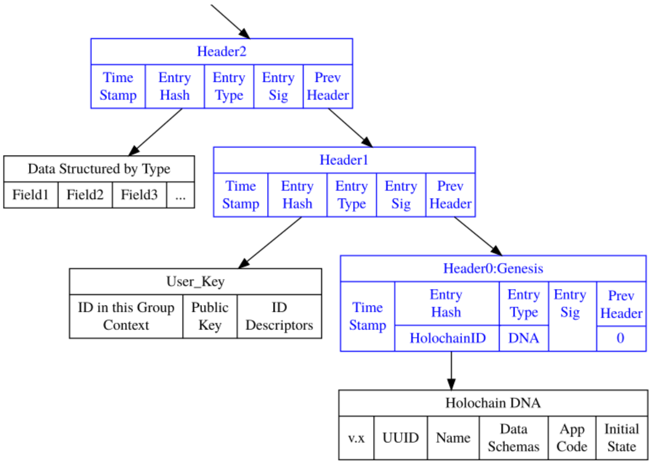

Figure 6: An example of a local chain [69].

4.1.2 Shared storage (DHT)

In order to describe how a DHT is used in Holochain, the general concept of a DHT is explained first.

4.1.2.1 Distributed Hash Table (DHT)

A distributed hash table (DHT) is a type of peer-to-peer distributed system designed to store data across multiple nodes [71]. It provides a lookup service similar to a hash table in that (key, value) pairs are stored in a DHT. This allows any participating node to efficiently retrieve the value associated with a given key [72]. A rather simplistic analogy is a telephone book where a user can retrieve a value (telephone number) by looking for the corresponding key (name). However, a DHT is, as the name suggest, distributed among many nodes. This creates the need for a routing layer in order for any node to locate the node that stores a particular key [73]. This routing layer distinguishes two types of DHTs: structured and unstructured DHTs.

In unstructured DHTs, lookup messages are sent to all nodes in the network, which results in poor performance. Structured DHTs, on the other hand, use routing tables to propagate messages among nodes to more efficiently find the relevant node [71]. The mechanics of how the routing table works, and how the table is updated as nodes join and leave the network, is a key differentiator between different DHT algorithms [73].

The responsibility for maintaining the mapping from keys to values is distributed among the nodes in such a way that a change in the set of participants causes a minimal amount of disruption. This allows a DHT to scale to extremely large numbers of nodes and to handle continual node arrivals, departures, and failures [72].

4.1.2.2 Holochain's implementation of a DHT

As mentioned in the previous section, every user maintains its own local hash chain per Holochain application or hApp. However, Holochain uses a DHT to store multiple redundant copies of each entry which allows data to be available even when the originator is offline and, most importantly, to improve security as each entry is saved in multiple locations. The distribution of an entry on the DHT happens by using a "gossip" protocol. In essence, every node spreads the message to some of their peers and these peers spread the message again on their turn. The data thus propagates slowly at first but then spreads at an exponential rate [74].

The number of redundant copies in the DHT is set by the resilience factor, configured in the DNA of the hApp. As this factor is increased, more copies are saved from one particular entry. Applications that require higher security or better failure tolerance can thus set this resilience factor to a higher value [75] [76].

It is important to note that every node only holds a small "shard" of the DHT and thus only carries a small part of the total data available in the network. This is in contrast with the Bitcoin blockchain where every full node needs to hold all the data [70]. This differentiation allows Holochain to be more scalable than the Bitcoin blockchain, since every new node contributes useful computation and storage resources to the platform [77]. Furthermore, as with the local source chain, hashing, timestamping and digital signatures are implemented in the DHT in order to create a secure, distributed, tamper-proof ledger [78].

4.1.2.3 Holochain's validating DHT

Holochain adds one more functionality to the DHT: it validates every entry that is added to it. This means that data cannot propagate on the network without first being validated by shared validation rules held by every node, just like every cell in your body has a copy of the same DNA [10]. These validation rules are the following:

(1) The receiving node confirms the provenance of the piece of data.
(2) The receiving node validates the signature of its author.
(3) The receiving node validates if the author has committed the data to their local chain.

If the data entry does not break any rules, the validator saves the data, marks it valid and signs a statement with his/her digital signature. This means that if someone hacked their code to behave differently, even if they colluded with others, the rest of the nodes on the DHT would not validate their altered behavior and they will have essentially just "forked" themselves out of being able to participate on that particular Holochain application [10]. Thus, all cooperating participants can detect modified or invalid data, spread evidence of corrupt actors or validators, and take steps to counteract threats. Also note that, as the entry is passed to more nodes in its neighborhood, it gathers more signatures attesting to its validity [76].

4.1.3 Application

A Holochain application, or hApp, is the third essential component of the Holochain technology. It is simply an application a user wants to run on the Holochain network, for example, Clutter, a peer-to-peer version of Twitter [79]. Every application can read from and write on every participating node's own local signed hash chain and the shared DHT [69].

4.1.3.1 DNA of the application

As mentioned before, every hApp has a set of validation rules, called DNA, which prescribes the rules for interacting with the network. This is depicted in the first two blocks of Figure 6, which are called the "genesis" entries. These two entries contain the following [76]:

(1) The hash of the DNA. Because the DNA constitutes the 'rules of play' for everyone in the app, this entry shows that you have seen and agree to abide by those rules.
(2) Your agent ID. This contains your public key as a record of your digital identity. The signatures on all subsequent entries must match this public key in order to be valid. This entry can also contain extra information necessary for gaining entry to the network, such as an invite code or proof of paid dues.

After these two genesis entries comes the app entries or user data. Remember that an entry on the local source chain cannot be modified once it's been committed. This is important, since this local source chain is a record of all the things a user has done in the hApp, and peers may need to check this record in order to validate an entry.

4.1.3.2 Immune system

Another security feature that Holochain has implemented, besides validating all entries on the DHT, is the so-called "immune system". Nodes look at their DHT, the various hApps and their respective DNA that they have. When certain actors are determined to be breaking DNA rules, nodes communicate this information to each other, and the bad actors are shut out of the Holochain network [80].

4.1.3.3 Malicious nodes

The security measures described above guarantee that if a user hacks the application in order to behave differently, even if they colluded with others, the rest of the nodes on the distributed hash table will not validate their altered behavior. Essentially, the malicious node(s) will have forked themselves out of the application [69]. In addition, if foul play is detected on a node's part, by propagating or validating bad data, that node is blocked, and a warning is sent to others. Bad validators can be easily detected since every node signs a statement when performing the checks before propagating the data.

For example, if a user wants to tweet something on Clutter, that tweet should comply with the DNA of Clutter. One of the rules in the DNA of the application can be that "every tweet on Clutter should have a maximum of 140 characters". If a user however alters the DNA by hacking the application to tweet a message with more than 140 characters, the data will be rejected by other nodes. The user thus has forked him/herself into application with a new local source chain.

As a result of these security measures, a participant in an application on Holochain can thus only write to the shared space if it is according to "terms of service" the user agreed to in the beginning. Every distributed application has its own DNA or rules for "consensus" and it is the DNA of a distributed application that guarantees that data being held in the shared distributed hash table can't be tampered with, counterfeited, or lost [69] [80].

4.1.3.4 "Consensus" in Holochain

Holochains don't manage consensus about some absolute perspective on data or sequence of events as in the case of blockchain. Instead, Holochain manages distributed data integrity. In other words, Holochains rely on consensus about the validation rules (DNA) which define that integrity[4] [81]. Peers then validate data that is shared on the network by verifying if the rules are adhered to. This radically reduces the computational overhead of every node, since these do not have to replicate all of the data [70]. Furthermore, a user does not need to trust anyone on the network, not the provider of the application nor any other person operating on that application, but only needs to agree with the shared protocols that make up the application itself. Application providers are thus responsible for the maintenance and security of the hApps they provide, but do not own the data of the users, since this data will be stored on the user's local chain and portions of it are spread out on the DHT.

4.1.3.5 Multi-party transactions

Interactions involving multiple parties, such as a currency transfer between two people, are signed by each party and committed to both of their own chains, and then shared to the distributed hash table by each party. In this DHT, nodes can confirm or reject the data by validating if the data is in line with the shared rules [69]. Note that each party signs the exact same transaction with links to each of their previous chain entries [81]. This "crossing" of chains assures users that even if the counterparty tries to alter their chain, the transaction is still published by others.

4.2 CHARACTERISTICS OF HOLOCHAIN

4.2.1 Benefits

Since several essential techniques from the blockchain technology are implemented into Holochain, Holochain enjoys from the same benefits as the Bitcoin technology.

4.2.1.1 Immutability

Data on the Holochain platform is immutable once written due to the cryptographic linking of entries by hashing the previous header into the current one. However, although it is not possible to delete data on the network, it is possible to tag a data with an entry "deleted". This will make the application ignore that data in the UI.

4.2.1.2 Append only and time-stamped

All records on Holochain are date and time stamped, ensuring a logical sequence of events. Both the agent's source chain and the DHT are append-only due to inclusion of the hash of the previous entry [74].

4.2.1.3 Secure

Holochain uses, just as blockchain, public key encryption in order to secure data on the network. This reduces the risk of data corruption and fraud. In addition, by implementing ground rules into the Holochain applications (called the DNA of the hApp) and letting

[4] In essence, every blockchain protocol stores rules. In Bitcoin, these rules are denoted in the version, mentioned in the block header.

nodes compare their DHT with their DNA, data can be validated by peers on a constant basis. Holochain thus does not manage a universal ledger of data and does not need to reach consensus about this single ledger. As a result, attacks on consensus are not vulnerabilities for Holochain. This includes majority attacks, such as the 51% attack, most Sybil attacks, attacker with high computing power, high energy consumption, selective dropping of transactions and more (Brock et al., 2018).

4.2.1.4 Open and transparent

The distributed hash table is, as the name implies, distributed among peers on the network. All peers can check and validate the data that is on this DHT, making the technology open and transparent.

4.2.2 Additional benefits

Due to the unique structure of Holochain, several additional benefits can be attributed to the technology. Holochain lists the following benefits on their website [77].

4.2.2.1 Scalable

Since Holochain does not manages consensus about data, no consensus mechanism is needed either. Instead, Holochain manages consensus about the DNA, or the ground rules by which to act on in a certain application. This allows users to validate entries themselves, instead of letting a "central" party (miners in the case of blockchain) check and validate the data. As a result, every user contributes useful computation and storage resources, making the performance scale linearly with new users [77].

4.2.2.2 Resilient

Holochain defines "resilience" as "the level of a network's capacity to hold itself in integrity as nodes leave, join or attempt to attack it" [74]. Since Holochain stores its data among all participants using a distributed hash table, there are no centralized failure points. An attacker thus needs to attack all participants storing a particular piece of information in order to alter it. Furthermore, since Holochain uses a distributed hash table, nodes can join or leave the network anytime. In the DHT, nodes communicate directly with each other using an encrypted protocol, maintaining redundancy and adapting quickly to failures and attacks. Holochain is therefore built for anti-fragility [77].

4.2.2.3 Empowering

The local source chain contains all of a particular user's data, and solely parts of it are saved on other nodes in the DHT. This means that hApps on the Holochain network will live exclusively on distributed networks of consumer-owned computers which do not need to interact with corporate servers. These corporations that own those servers thus won't be able to strip-mine your personal data as it passes through their corporate computers, because your data won't pass through those computers [82]. As a result, users are in charge of their identity, data and infrastructure [77].

4.2.2.4 Evolvable

Most blockchains, including Bitcoin, have a system that deploys a currency in a decentralized architecture. However, over time, the system has become more centralized due to the increase of mining farms and pools, which now control most of the computing power. As a result, a small portion of the participants control the majority of the system. The ability for these blockchains to adapt and evolve is therefore dependent on this small group. As to be truly decentralized, a system thus not only needs to include a decentralized issuance, operation and accounting, but also the means to decentralize decision making about the ongoing evolution of the code itself [83]. Holochain, as opposed to Bitcoin, supports fast and agile development by creating microservices that can be bridged together. Applications on Holochain are best implemented as an integrated collection of standalone microservices. Any solution can become a valuable new component of the ecosystem without compromising the original solution. As a result, Holochain applications can adapt and evolve with changing needs [84].

4.2.2.5 Fast and lean

Participants on a certain Holochain application are in consensus about the rules of that application, not about data that is shared on it. This allows peers to validate each other, instead of making one central party (miners in the case of Bitcoin) responsible for this process. As a result, speed, latency, throughput, efficiency and cost of hardware are drastically improved in Holochain [83]. In benchmarking tests against Ethereum, the technology has proven to be 10,000 times faster and cheaper, and that's a conservative estimate [70]. Furthermore, there is no need to wait 10 minutes for a transaction to be committed [83].

4.2.2.6 Flexible

In order to change the system of a public blockchain platform, such as Bitcoin, a soft or hard fork is required. On Holochain, however, hApp developers are allowed to choose and implement their own rules as long as they do not contradict DNA. It's important to note that DNA is inherent to each hApp. In other words, each hApp has its own DNA or rules for "consensus" [80]. Holochain is thus a versatile framework for building interconnected public, private, and hybrid networks. With very few assumptions baked in, a developer is free to design his/her network to suit his/her own needs.

4.2.3 Limitations

Although Holochain offers multiple more advantages than Bitcoin, it still has some limitations. These are described below [10].

4.2.3.1 Responsibility on developers

With the increased flexibility Holochain offers to developers also comes responsibility. Since every distributed application has its own DNA, developers are responsible to set DNA before building out a hApp ecosystem to ensure that the hApp runs smoothly. This could prove dangerous, as seen in the case of Ethereum. While developers have more free reign in designing their Ethereum-based hApp sand smart contracts, this has led to numerous issues, such as The DAO hack, Parity wallet hacks and other mishaps, as developers have been unable to develop their solutions properly [80].

4.2.3.2 Large files

Holochain is made for small- and large-scale social coordination, such as social networks, supply chains and mutual credit cryptocurrencies. It can be thought of a database for structured data storage, instead of a file system. As a result, it is not made for token-based currencies and transfer of large files [70]. Essentially, since all data is spread out on the DHT, nobody on the network wants to be forced to load and host another user's large data files [10].

4.2.3.3 Data privacy

Although governance, resilience and privacy are configurable to the requirements of the application, data on Holochain is, as in Bitcoin, immutable [84]. Once data is added to the distributed hash table, there is no way to delete it. Holochain is aware of this issue, however, it is seen as a feature, rather than a vulnerability (Brock et al., 2018). The Holochain team therefore openly shares to assume that data is not private on Holochain. However, privacy on Holochain could be improved in the future by adding an anonymization layer, such as TOR, but it is not natively included into the technology [77].

Note, however, that data is stored on a user's local hash chain and "chunks" of this data are spread on the DHT as to provide a security and redundancy mechanism. Only the user's local hash chain thus contains the complete set of his/her own data. Because of this design, Holochain is natively supporting European GDPR regulations [84].

5 RESULTS

In this section, the Bitcoin blockchain and Holochain are compared in terms of scalability, data privacy and interoperability.

5.1 SCALABILITY

In the network context, scalability is usually measured by how fast transactions are processed, usually denoted in transactions per second (tps). However, scalability covers additional measures as well, such as the data packet size, the network latency and, in the case of blockchain networks, other features, such as sharding, staking and bridges to other blockchains [85]. However, in this paper, scalability will be measured by the processing speed of transactions (tps).

5.1.1 Bitcoin blockchain

As mentioned previously, the Bitcoin network is able to process roughly 7 tps. This is drastically below the performance of the VISA network, which can process thousands of transactions per second (Chen et al., 2020). In order for the Bitcoin network to increase its throughput, it can increase the block size, which is currently limited to 4 MB, and/or increase the block generation time, that is the amount of time it takes for adding a new block, which is set at 10 minutes. There are thus three possibilities to increase the throughput of the Bitcoin network:

(1) Increase the block size.
(2) Decrease the block generation time.
(3) A combination of (1) and (2).

However, none of the scenarios above can achieve similar transaction speeds as the VISA network due to a third, uncontrolled factor: the relay time needed to broadcast a new block to every node on the Bitcoin network [86]. This relay time can be increased if all the peers on the network update their bandwidth, however, that is the responsibility of every peer on the network itself.

In addition to this relay time, both increasing the block size and decreasing the block generation time comes with other costs as well, such as security, decentralization, size and latency issues. It can therefore be concluded that the Bitcoin network, and all similar blockchain protocols, have an inherent scalability issue.

5.1.2 Holochain

As explained earlier, Holochain reaches consensus about the rules of the application, which allows peers to validate each other's data. As a result, Holochain's performance scales linearly with new users, since every user contributes useful computation and storage resources [77]. This is in stark contrast with Bitcoin where there is consensus about the data that is transmitted. Miners are responsible for solving the mathematical puzzle and thus decide what information becomes part of the block and the universal ledger. The Bitcoin blockchain therefore does not scale when new users enter the network.

However, due to this nature of Holochain, it is not possible to give a conclusive answer to the question "What is the tps limit of Holochain?" since there is no single bottleneck. The Holochain team compares it to asking, "how many words can humanity speak per second?" "Well, with every human being born, that number increases. Same for Holochain" [81].

Nevertheless, the Holochain did perform benchmarks on a Holochain application called "Holo", comparing the price of computation to the Holo app and Ethereum, which is the second most popular blockchain protocol according to market capitalization [1]. The results of these benchmarks are astonishing: Holo is at least 10 000 times faster and cheaper than Ethereum. Moreover, the team believes it will end up closer to 100 000 times faster [70] [87].

5.2 DATA PRIVACY

The internet allows users to access vast amounts of data. According to research, in 2018, 2.5 quintillion (10^{18}) bytes of data was created every day and the total amount of data in the world was estimated to be 44 zetta (10^{21}) bytes at the dawn of 2020 [78] [88] [89]. However, most of this data is currently stored in centralized data servers, which are a collection of servers and computing systems. These systems are vulnerable for attacks and, as a result, data incidents, which can be defined as events involving misuses of individuals' personal information, appear regularly (Acquisti et al., 2006). These incidents have consequences for both companies and customers (Gimpel et al., 2018). Blockchain and Holochain both offer a solution to store data in a decentralized manner. In this section, both the technology's performance related to data privacy is investigated.

5.2.1 Bitcoin blockchain

Blockchain is a distributed database system in which data is completely transparent to anyone on the network. This allows users to control the entire process of their transactions in an open manner (Woodside & Jr, 2017). Bitcoin users operate on the network by using a pair of cryptographic keys: a private and a public key. Bitcoin transactions are thus not truly anonymous but rather pseudonymous, in that each transaction specifies account information (the user's public key) albeit without personal names, and the blockchain publishes transactions by that user identifier (Böhme et al., 2015).

However, according to a study by Goldfeder S. et al, cryptocurrency users can be deanonymized by third web trackers, which store information about user purchases for purposes of advertising and analytics. These trackers typically possess enough information about the purchase to uniquely identify the transaction on the blockchain, link it to the user's cookie and further to the user's real identity (Goldfeder et al., 2017). In addition, statistical techniques and pattern analysis can profile and reveal up to 60% of the Bitcoin users, according to a study by Tsukerman in 2015 (Dumitrescu, 2017). Other studies have provided additional experimental evidence on the lack of anonymity in the Bitcoin network as well (Feld et al., 2014; Koshy et al., 2014). It thus seems that, although there is no direct relationship between wallets and individuals, user anonymity can be compromised (Reyna et al., 2018).

Furthermore, there are also data privacy issues related to the safeguarding of the private key. If one's private key is acquired or stolen, no third party can recover it. Consequently, all the assets this person owns in the blockchain will vanish, and it will be nearly impossible to identify the thief (Efanov & Roschin, 2018).

5.2.2 Holochain

Holochain uses the same dual-key cryptography technique as Bitcoin. As a result, users on the Holochain are, just as on the Bitcoin blockchain, pseudonymous instead of truly anonymous. However, the founders of Holochain see this as a strength and even mention on their website to assume your data is not private [10] [78]. Nonetheless, since Holochain uses dual-key cryptography in a similar way as the Bitcoin blockchain, it suffers from the same issues related to this technology, such as keeping your private key safe and the possibility of someone linking a user's public key to his/her real identity.

Nonetheless, since data on Holochain is stored on a user's local hash chain and "chunks" of that data are spread on the DHT, only the user him/herself holds all of his/her own data. This results in Holochain natively supporting European GDPR regulations [84].

It can thus be concluded that Holochain offers a slight improvement over the Bitcoin blockchain in terms of data privacy [90], but some issues due to the limitations of public key cryptography still remain.

5.3 INTEROPERABILITY

In short, interoperability is the ability to freely share information across (blockchain) systems. In a fully interoperable environment, various different blockchains are able communicate easily with each other, without the need for an outside intermediary [91] [5].

5.3.1 Bitcoin blockchain

As mentioned before, transformative blockchain applications are still not commercially available and few organizations have progressed their blockchain solutions beyond the feasibility or prototype stage. One of the reasons of this slow migration toward blockchain in the financial industry is the lack of a common architecture across industry and integration or communication with transactional based systems (Hughes et al., 2019). This opinion is also shared by Kumar: "Blockchain is evolving in many ecosystems, such as Hyperledger and Ethereum, but there needs to be a native way to integrate blockchains that would allow, for example, a transaction on Hyperledger to invoke information from Ethereum." (Underwood, 2016). However, other aspects, such as anonymity, decentralization and scalability have initially been investigated, effects of interoperability, (un-) permissioned blockchains, restricted data access, consensus mechanisms and modularity are mostly disregarded (Risius & Spohrer, 2017). Interoperability thus requires extensive further research to analyze solutions to interblockchain communication and integration with transactional systems (Hughes et al., 2019).

5.3.2 Holochain

Holochain is, as opposed to Bitcoin, not a monolithic network. Instead, Holochain can be better described as a configurable framework for building interoperable public, private and hybrid networks. Application developers are allowed to configure settings according to the specifications of their particular use case. In fact, almost any blockchain solution can be built on Holochain and since the underlying framework of the applications is the same, these solutions can talk to each other, allowing data to be shared to each other and/or to the outside world. This allows enterprises with a working system to extend its capacity at the margins using Holochain and gradually replacing existing parts of the system without the kind of service disruptions the enterprise would experience when jumping to traditional blockchains. This enables the corporations to profit from the benefits, discussed earlier, offered by Holochain without sacrificing business performance while transitioning. The final result of this transition will be an ecosystem of small, versatile single-purpose distributed applications, which combined create a new and more robust solution [77] [84].

6 CONCLUSION

It is noted that, although blockchains are listed as a "disrupting technology", no transformative blockchain applications are commercially available and most organizations barely pass the prototype stage. As an answer to this situation, Holochain, an agent-centric 'blockchain', has been developed by three pioneers: Eric Harris-Braun, Arthur Brock and Nicolas Luck. This paper has presented an explorative introduction to this technology as well as compared the performance of the technology to three issues pervasive through all blockchains: scalability, data privacy and interoperability.

First, Holochain is more scalable since it does not pose a limit on the amount of transactions that can be processed per second. This is due to the fact that Holochain does not reach consensus about the data, but on the rules. As a result, performance scales linearly with new users, since every user contributes useful computation and storage resources. Bitcoin, on the other hand, currently has a transaction limit of 7 tps due to its working structure.

Second, data is stored in a slightly more secure and private manner on the Holochain network since only the local hash chain of the user stores the complete set of his/her personal data. Due to this design, Holochain natively supports the GDPR regulations. However, it is still susceptible to the same privacy issues related to dual key cryptography as Bitcoin.

Third, Holochain is considered more interoperable than the Bitcoin blockchain as it is not a monolithic network, but rather a framework for building applications that can be configured according to the specific needs of that particular application. This allows an enterprise to create distributed applications at the margins of their current working system, and slowly replace more parts with a Holochain alternative. The final result is then a compound solution of several distributed applications, which in the end, create a more robust and evolvable solution.

7 FUTURE RESEARCH AND LIMITATIONS

This paper aims to give an explorative introduction to a new sort of Blockchain called Holochain. However, the paper should be seen within its limitations.

First, although several conclusions are drawn in this paper, it should be noted that this a qualitative paper. Quantitative (case) studies should be performed in order to statistically back the conclusions in this paper.

Secondly, this paper compares Holochain to the Bitcoin protocol. However, multiple blockchain protocols exist, some of them featuring new technological features to solve several issues inherent to the Bitcoin protocol. This led to the development of blockchain 2.0 applications, which added a coding layer, and blockchain 3.0 applications, which can be described as "distributed cloud computing networks". The most popular blockchain 2.0 application is the Ethereum protocol, some upcoming blockchain 3.0 platforms are Cordano, IOTA and the Lightning Network. Carrying out a comparison between these platforms and Holochain will bring about a more general conclusion to the performance of the Holochain network regarding scalability, data privacy and interoperability.

Third, Holochain is a very new concept (Holochain whitepaper was released in 2018). As a result, not much literature exists on the web, besides that from crypto-enthusiasts and from the Holochain team itself. More thorough documentation is needed in order to extend the amount of academic research that can be done on the technology.

8 ACKNOWLEDGEMENTS

I would like to thank prof. dr. Benoît Depaire, my thesis promotor, for the support during the year. Although I first contacted him in December, 3 months after the start of the semester, he did not judge me for being late. Instead, he helped me develop a plan on how to tackle the thesis. I hope I did not let him down with this submission.

I would also like to thank my parents for giving me the opportunity to get my second master's degree, after graduating as an Industrial Engineer.

9 REFERENCES

9.1 ACADEMIC JOURNALS, CONFERENCE PAPERS, BOOKS AND DOCUMENTS

Acquisti, A., Friedman, A., & Telang, R. (2006). *Is there a cost to privacy breaches? An event study*. 94. http://aisel.aisnet.org/icis2006/94

Ahmed, V., Opoku, A., & Aziz, Z. (Eds.). (2016). *Research methodology in the built environment: A selection of case studies*. Routledge, Taylor & Francis Group.

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the open blockchain* (Second edition). O'Reilly.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, *29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213

Brock, A., Atkinson, D., Friedman, E., Harris-Braun, E., McGuire, E., M. Russel, J., Perrin, N., Luck, N., & Harris-Braun, W. (2018). *Holo Green Paper (Arthur Brock, et al.).pdf*. https://files.holo.host/2018/03/Holo-Green-Paper.pdf

Buterin, V. (2013). *A next generation smart contract & decentralized application platform*. https://github.com/ethereum/wiki/wiki/White-Paper

Chase, B., & MacBrough, E. (2018). Analysis of the XRP Ledger Consensus Protocol. *ArXiv:1802.07242 [Cs]*. http://arxiv.org/abs/1802.07242

Chen, L., Xu, L., Gao, Z., Kasichainula, K., & Shi, W. (2020). Nonlinear Blockchain Scalability: A Game-Theoretic Perspective. *ArXiv:2001.08231 [Cs]*. http://arxiv.org/abs/2001.08231

Dumitrescu, G. C. (2017). Bitcoin – A Brief Analysis of the Advantages and Disadvantages. *Global Economic Observer*, *5*(2), 63–71.

Efanov, D., & Roschin, P. (2018). The All-Pervasiveness of the Blockchain Technology. *Procedia Computer Science*, *123*, 116–121. https://doi.org/10.1016/j.procs.2018.01.019

Feld, S., Schönfeld, M., & Werner, M. (2014). Analyzing the Deployment of Bitcoin's P2P Network under an AS-level Perspective. *Procedia Computer Science*, *32*, 1121–1126. https://doi.org/10.1016/j.procs.2014.05.542

Gimpel, H., Kleindienst, D., Nüske, N., Rau, D., & Schmied, F. (2018). The upside of data privacy – delighting customers by implementing data privacy measures. *Electronic Markets*, *28*(4), 437–452. https://doi.org/10.1007/s12525-018-0296-3

Goethals, G. R., Sorenson, G. J., & MacGregor Burns, J. (2004). *Qualitative Research*. Sage.

Goldfeder, S., Kalodner, H., Reisman, D., & Narayanan, A. (2017). When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. *ArXiv:1708.04748 [Cs]*. http://arxiv.org/abs/1708.04748

Harris-Braun, E., Luck, N., & Brock, A. (2018). *Holochain—Scalable agent-centric distributed computing.pdf*. https://github.com/holochain/holochain-proto/blob/whitepaper/holochain.pdf

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, *49*, 114–129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005

Koshy, P., Koshy, D., & McDaniel, P. (2014). An Analysis of Anonymity in Bitcoin Using P2P Network Traffic. In N. Christin & R. Safavi-Naini (Eds.), *Financial Cryptography and Data Security* (Vol. 8437, pp. 469–485). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-45472-5_30

Kube, N. (2018). Daniel Drescher: Blockchain basics: a non-technical introduction in 25 steps: Apress, 2017, 255 pp, ISBN: 978-1-4842-2603-2. *Financial Markets and Portfolio Management*, *32*(3), 329–331. https://doi.org/10.1007/s11408-018-0315-6

Longo, F., Nicoletti, L., Padovano, A., d'Atri, G., & Forte, M. (2019). Blockchain-enabled supply chain: An experimental study. *Computers & Industrial Engineering*, *136*, 57–69. https://doi.org/10.1016/j.cie.2019.07.026

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications*, *125*, 251–279. https://doi.org/10.1016/j.jnca.2018.10.019

McGhin, T., Choo, K.-K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*, 62–75. https://doi.org/10.1016/j.jnca.2019.02.027

Meyer, T., Kuhn, M., & Hartmann, E. (2019). Blockchain technology enabling the Physical Internet: A synergetic application framework. *Computers & Industrial Engineering*, *136*, 5–17. https://doi.org/10.1016/j.cie.2019.07.006

Nakamoto, S. (n.d.). *Bitcoin: A Peer-to-Peer Electronic Cash System*. 9.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. 9.

Naor, M., & Yung, M. (1989). Universal one-way hash functions and their cryptographic applications. *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing - STOC '89*, 33–43. https://doi.org/10.1145/73007.73011

Pierce, B., Collins, R., & Sellars, C. (2016). *Fiat currencies on the Bitcoin blockchain.pdf*. https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046

Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There. *Business & Information Systems Engineering*, *59*(6), 385–409. https://doi.org/10.1007/s12599-017-0506-0

Sas, C., & Khairuddin, I. E. (2015). Exploring Trust in

Bitcoin Technology: A Framework for HCI Research. *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction on - OzCHI '15*, 338–342. https://doi.org/10.1145/2838739.2838821

Schepers, D. (2018). *The Business Value of Blockchain* [Theses and Dissertations, UHasselt]. http://hdl.handle.net.bib-proxy.uhasselt.be/1942/27021

Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, *86*, 650–655. https://doi.org/10.1016/j.future.2018.04.060

Sun, J., Yan, J., & Zhang, K. Z. K. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, *2*(1), 26. https://doi.org/10.1186/s40854-016-0040-y

Tang, Y., Xiong, J., Becerril-Arreola, R., & Iyer, L. (2019). Ethics of blockchain: A framework of technology, applications, impacts, and research directions. *Information Technology & People*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/ITP-10-2018-0491

Tönnissen, S., & Teuteberg, F. (2020). Analysing the impact of blockchain-technology for operations and supply chain management: An explanatory model drawn from multiple case studies. *International Journal of Information Management*, *52*, 101953. https://doi.org/10.1016/j.ijinfomgt.2019.05.009

Treiblmaier, H. (2019). Toward More Rigorous Blockchain Research: Recommendations for Writing Blockchain Case Studies. *Frontiers in Blockchain*, *2*, 3. https://doi.org/10.3389/fbloc.2019.00003

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15–17. https://doi.org/10.1145/2994581

Vujicic, D., Jagodic, D., & Randic, S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, 1–6. https://doi.org/10.1109/INFOTEH.2018.8345547

Wamba, S. F., & Queiroz, M. M. (2020). Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities. *International Journal of Information Management*, *52*, 102064. https://doi.org/10.1016/j.ijinfomgt.2019.102064

Woodside, J. M., & Jr, F. K. A. (2017). *Blockchain Technology Adoption Status and Strategies*. *26*(2), 30.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLOS ONE*, *11*(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain Technology Use Cases in Healthcare. In *Advances in Computers* (Vol. 111, pp. 1–41). Elsevier. https://doi.org/10.1016/bs.adcom.2018.03.006

Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, *10*(4), 983–994. https://doi.org/10.1007/s12083-016-0456-1

9.2 WEBDOCUMENTS

[1] Coinmarketcap, "Top 100 Cryptocurrencies by Market Capitalization," CoinMarketCap, [Online]. Available: https://coinmarketcap.com. [Accessed 24 April 2020].

[2] BitcoinCash, "THE BITCOIN CASH ROADMAP," BitcoinCash, [Online]. Available: https://www.bitcoincash.org/roadmap.html. [Accessed 24 April 2020].

[3] J. Vincent, "Bitcoin consumes more energy than Switzerland, according to new estimate," The Verge, 4 July 2019. [Online]. Available: https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison. [Accessed 27 April 2020].

[4] Digiconomist, "Bitcoin Energy Consumption Index," Digiconomist, 27 April 2020. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption. [Accessed 27 April 2020].

[5] A. Brock and J. Russel, "How does Holochain work?," YouTube, 10 April 2018. [Online]. Available: https://www.youtube.com/watch?v=XH2dV33shxE. [Accessed 26 April 2020].

[6] D. Cearly, "Gartner Top 10 Strategic Technology Trends for 2020," Gartner, 21 October 2019. [Online]. Available: https://www.youtube.com/watch?v=6HzdOkPPPRU&feature=emb_title. [Accessed 25 April 2020].

[7] K. Panetta, "Gartner Top 10 Strategic Technology Trends for 2020," Gartner, 21 October 2019. [Online]. Available: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020. [Accessed 25 April 2020].

[8] M. Andress, "Top Tech Trends To Watch In 2020," Forbes, 23 January 2020. [Online]. Available: https://www.forbes.com/sites/mergermarket/2020/01/23/top-tech-trends-to-watch-in-2020/#5aab9a744d1f. [Accessed 25 April 2020].

[9] S. Buchholz and B. Briggs, "Tech Trends 2020," Deloitte, 15 January 2020. [Online]. Available: https://www2.deloitte.com/us/en/insights/focus/tech-trends.html. [Accessed 25 April 2020].

[10] Ceptr, "Holochains for Distributed Data Integrity," Ceptr, [Online]. Available: http://ceptr.org/projects/holochain. [Accessed 26 April 2020].

[11] E. Harris-Braun, "Why the "currency" in the the meta-currency project?," New Currency Frontiers, 25 March 2009. [Online]. Available: http://blog.newcurrencyfrontiers.com/2009/03/why-currency-in-the-meta-currency.html. [Accessed 26 April 2020].

[12] Amanda DHT, "Junto: A New Breed of Social Media Powered by Holochain," Holochain, 30 January 2019. [Online]. Available: https://blog.holochain.org/junto--a-new-breed-of-social-media-powered-by-holochain/. [Accessed 25 April 2020].

[13] Amanda DHT, "RedGrid: Building the Internet of Energy Platform," Holochain, 20 March 2019. [Online]. Available: https://blog.holochain.org/redgrid--building-the-internet-of-energy-platform/. [Accessed 25 April 2020].

[14] D. Saada, "Holochain Developers Growing as a Vibrant and Self-Sustained Community," The Currency Analytics, 14 December 2019. [Online]. Available: https://thecurrencyanalytics.com/8820/holochain-developers-growing-as-a-vibrant-and-self-sustained-community/. [Accessed 2020 April 2020].

[15] N. Thattamparambil, "How to choose the research methodology best suited for your study," Editage, 17 February 2020. [Online]. Available: https://www.editage.com/insights/how-to-choose-the-research-methodology-best-suited-for-your-study. [Accessed 26 April 2020].

[16] M. Nimfuehr, "The Amazing Story of Cryptocurrencies Before Bitcoin," Hackernoon, 5 November 2018. [Online]. Available: https://hackernoon.com/the-amazing-story-of-cryptocurrencies-before-bitcoin-fe1b0e55155b. [Accessed 27 April 2020].

[17] H. Agrawal, "What is Double Spending & How Does Bitcoin Handle It?," Coinsutra, 6 November 2019. [Online]. Available: https://coinsutra.com/bitcoin-double-spending/. [Accessed 27 April 2020].

[18] Bitcoin.org, "Bitcoin Developer Reference," Bitcoin.org, [Online]. Available: https://bitcoin.org/en/developer-reference#block-chain. [Accessed 27 April 2020].

[19] D. Canellis, "Here's why Bitcoin's blockchain has blocks that go over the 1MB limit," The Next Web, 12 July 2018. [Online]. Available: https://thenextweb.com/hardfork/2018/07/12/bitcoin-block-size/. [Accessed 29 April 2020].

[20] Blockchain, "Average Block Size (MB)," Blockchain, 1 May 2020. [Online]. Available: https://www.blockchain.com/charts/avg-block-size. [Accessed 1 May 2020].

[21] N. Reiff, "Blockchain Explained," Investopedia, 1 February 2020. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp. [Accessed 1 May 2020].

[22] J. Frankenfield, "Merkle Tree," Investopedia, 18 February 2020. [Online]. Available: https://www.investopedia.com/terms/m/merkle-tree.asp. [Accessed 27 April 2020].

[23] Ivan On Tech, "What is inside a Bitcoin block? Programmer explains.," YouTube, 16 May 2017. [Online]. Available: https://www.youtube.com/watch?v=qLM-UC_eqIY. [Accessed 27 April 2020].

[24] J. Frankenfield, "Hash," Investopedia, 15 August 2019. [Online]. Available: https://www.investopedia.com/terms/h/hash.asp. [Accessed 27 April 2020].

[25] Xorbin, "SHA-256 hash calculator," Xorbin, [Online]. Available: https://xorbin.com/tools/sha256-hash-calculator. [Accessed 27 April 2020].

[26] N. Reiff, "How does a block chain prevent double-spending of Bitcoins?," Investopedia, 24 January 2020. [Online]. Available: https://www.investopedia.com/ask/answers/061915/how-does-block-chain-prevent-doublespending-bitcoins.asp. [Accessed 27 April 2020].

[27] Y. Zuehlke, "A clarification on the perpetual discussion of Bitcoin's timestamp," Hackernoon, 23 January 2019. [Online]. Available: https://hackernoon.com/a-clarification-on-the-perpetual-discussion-of-bitcoins-timestamp-5597859a9193. [Accessed 28 April 2020].

[28] O. Contis, "Immutability on Blockchain and Proof of Existence," Medium, 23 April 2019. [Online]. Available: https://medium.com/coinmonks/immutability-on-blockchain-and-proof-of-existence-f047ea7622bd. [Accessed 27 April 2020].

[29] Dotwallet, "What is Bitcoin Timestamp? Can it be changed?," Dotwallet, 04 April 2019. [Online]. Available: https://www.dotwallet.com/en/article/169. [Accessed 27 April 2020].

[30] G. Konstantopoulos, "Understanding Blockchain Fundamentals, Part 2: Proof of Work & Proof of Stake," Medium, 8 December 2017. [Online]. Available: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb. [Accessed 27 April 2020].

[31] M. Thake, "What is Proof-of-Work (PoW)?," Medium, 2 June 2018. [Online]. Available: https://medium.com/nakamoto/what-is-proof-of-work-pow-2574ddebf916. [Accessed 27 April 2020].

[32] J. D. Cook, "What is proof-of-work?," John D. Cook Consulting, 11 November 2018. [Online]. Available: https://www.johndcook.com/blog/2018/11/11/proof-of-work/. [Accessed 27 April 2020].

[33] H. Sharma, "Proof of 'What?' Series-Proof of Work(PoW)," Cutting Edge Visionaries, 4 January 2020. [Online]. Available: https://www.cevgroup.org/proof-of-what-series-proof-of-workpow/. [Accessed 27 April 2020].

[34] S. Verma, "Proof Of Work - A Puzzle for the new economy," Medium, 9 May 2018. [Online]. Available: https://medium.com/coinmonks/proof-of-work-a-puzzle-for-the-new-economy-552cb0f1cf45. [Accessed 27 April 2020].

[35] A. Tar, "Proof-of-Work, Explained," Cointelegraph, 17 January 2018. [Online]. Available: https://cointelegraph.com/explained/proof-of-work-explained. [Accessed 27 April 2020].

[36] A. Bulkin, "Explaining blockchain—how proof of work enables trustless consensus," Keeping Stock, 3 May 2016. [Online]. Available: https://keepingstock.net/explaining-blockchain-how-proof-of-work-enables-trustless-consensus-2abed27f0845. [Accessed 27 April 2020].

[37] M. Kapilov, "Why Today's 16% Fall in BTC Mining Difficulty May Cause the Price to Plunge," Cointelegraph, 25 March 2020. [Online]. Available: https://cointelegraph.com/news/why-todays-btc-difficulty-adjustment-may-cause-the-price-to-plunge. [Accessed 27 April 2020].

[38] G. Walker, "Blockchain," Learn Me A Bitcoin, 4 September 2019. [Online]. Available: https://learnmeabitcoin.com/guide/blockchain. [Accessed 28 April 2020].

[39] A. Grigorean, "Latency and finality in different cryptocurrencies," Hackernoon, 1 May 2018. [Online]. Available: https://hackernoon.com/latency-and-finality-in-different-cryptocurrencies-a7182a06d07a. [Accessed 29 April 2020].

[40] E. Hong, "How Does Bitcoin Mining Work?," Investopedia, 26 March 2020. [Online]. Available: https://www.investopedia.com/tech/how-does-bitcoin-mining-work/. [Accessed 28 April 2020].

[41] A. Hertig, "Bitcoin Halving, Explained," Coindesk, 6 April 2020. [Online]. Available: https://www.coindesk.com/bitcoin-halving-explainer. [Accessed 28 April 2020].

[42] J. Frankenfield, "Satoshi," Investopedia, 2 October 2019. [Online]. Available: https://www.investopedia.com/terms/s/satoshi.asp. [Accessed 28 April 2020].

[43] A. Batabyal, "Bitcoin Halving 2020 | Bitcoin Halving Explained," Coinswitch, 26 December 2019. [Online]. Available: https://coinswitch.co/news/bitcoin-halving-2020-bitcoin-halving-explained-read-more. [Accessed 28 April 2020].

[44] M. Beedham, "All you need to know about Bitcoin network nodes," The Next Web, 1 March 2019. [Online]. Available: https://thenextweb.com/hardfork/2019/03/01/bitcoin-blockchain-nodes-network/. [Accessed 29 April 2020].

[45] O'Reilly online learning, "Chapter 6. The Bitcoin Network," O'Reilly online learning, [Online]. Available: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch06.html. [Accessed 29 April 2020].

[46] Bitcoin.org, "Running A Full Node," Bitcoin, [Online]. Available: https://bitcoin.org/en/full-node#what-is-a-full-node. [Accessed 29 April 2020].

[47] Bitcoin Charts, "Bitcoin transaction size," Bitcoin, 1 May 2020. [Online]. Available: https://charts.bitcoin.com/btc/chart/transaction-size#5ma4. [Accessed 1 May 2020].

[48] N. Acheson, "Learn Bitcoin," Coindesk, 26 January 2018. [Online]. Available: https://www.coindesk.com/learn/bitcoin-101/what-is-bitcoin. [Accessed 1 May 2020].

[49] D. Leon, "Why Do I Need a Public and Private Key on the Blockchain?," WeTrustIO, 30 January 2017. [Online]. Available: https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76. [Accessed 1 May 2020].

[50] S. Haig, "Bitcoin Block Size, Explained," Cointelegraph, 24 July 2019. [Online]. Available: https://cointelegraph.com/explained/bitcoin-block-size-explained. [Accessed 29 April 2020].

[51] Bitcoin.com, "Blockchain Size," Bitcoin.com, 29 April 2020. [Online]. Available: https://charts.bitcoin.com/btc/chart/blockchain-size#5ma4. [Accessed 29 April 2020].

[52] D. Canellis, "Bitcoin has nearly 100,000 nodes, but over 50% run vulnerable code," The Next Web, 6 May 2019. [Online]. Available: https://thenextweb.com/hardfork/2019/05/06/bitcoin-100000-nodes-vulnerable-cryptocurrency/. [Accessed 29 April 2020].

[53] J. Young, "The Centralization Issue of Scaling BTC Solely by Block Size Increase," News BTC, 2018. [Online]. Available: https://www.newsbtc.com/2017/11/12/61408/. [Accessed 29 April 2020].

[54] M. Orcutt, "Once hailed as unhackable, blockchains are now getting hacked," Technology Review, 19 February 2019. [Online]. Available: https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/. [Accessed 30 April 2020].

[55] Coinwarz, "Bitcoin Difficulty Chart," Coinwarz, 28 April 2020. [Online]. Available: https://www.coinwarz.com/mining/bitcoin/difficulty-chart. [Accessed 28 April 2020].

[56] Coinsutra, "Explaining Hash Rate Or Hash Power In Cryptocurrencies," Coinsutra, 6 August 2019. [Online]. Available: https://coinsutra.com/hash-rate-or-hash-power/. [Accessed 28 April 2020].

[57] Coinwarz, "Bitcoin Hashrate Chart," Coinwarz, 30 April 2020. [Online]. Available: https://www.coinwarz.com/mining/bitcoin/hashrate-chart. [Accessed 30 April 2020].

[58] C. Kim, "The Rise of ASICs: A Step-by-Step History of Bitcoin Mining," Coindesk, 26 April 2020. [Online]. Available: https://www.coindesk.com/rise-of-asics-bitcoin-mining-history. [Accessed 29 April 2020].

[59] Mining Wholesale, "Innosilicon A10 Pro (5G) ETHMaster (500Mh)," Mining Wholesale, [Online]. Available: https://miningwholesale.eu/product/innosilicon-a10-pro-5g-ethmaster-500mh/. [Accessed 30 April 2020].

[60] S. Seth, "How Do Cryptocurrency Mining Pools Work?," Investopedia, 20 February 2018. [Online]. Available: https://www.investopedia.com/tech/how-do-mining-pools-work/. [Accessed 30 April 2020].

[61] F2Pool, "Bitcoin Mining Pools: 101," Medium, 17 March 2020. [Online]. Available: https://medium.com/f2pool/bitcoin-mining-pools-101-237fe2d25e9. [Accessed 30 April 2020].

[62] J. Frankenfield, "What Is a 51% Attack?," Investopedia, 6 May 2019. [Online]. Available: https://www.investopedia.com/terms/1/51-attack.asp. [Accessed 30 April 2020].

[63] Emerging Technology from the arXiv , "Bitcoin Transactions Aren't as Anonymous as Everyone Hoped," MIT Technology Review, 23 August 2017. [Online]. Available: https://www.technologyreview.com/2017/08/23/149531/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/. [Accessed 1 May 2020].

[64] N. Reiff, "Bitcoin vs. Bitcoin Cash: What Is the Difference?," Investopedia, 8 January 2020. [Online]. Available: https://www.investopedia.com/tech/bitcoin-vs-bitcoin-cash-whats-difference/. [Accessed 30 April 2020].

[65] N. Reiff, "A History of Bitcoin Hard Forks," Investopedia, 25 June 2020. [Online]. Available: https://www.investopedia.com/tech/history-bitcoin-hard-forks/. [Accessed 30 April 2020].

[66] N. Reiff, "The 10 Most Important Cryptocurrencies Other Than Bitcoin," Investopedia, 8 January 2020. [Online]. Available: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/. [Accessed 30 April 2020].

[67] B. Peh, "What are Public, Private and Hybrid Blockchains?," Medium, 10 November 2018. [Online]. Available: https://medium.com/@blockchain101/what-are-public-private-and-hybrid-blockchains-e01d6e21eb41. [Accessed 29 April 2020].

[68] O. Dale, "A Beginner's Guide to Holochain: A Framework for Peer-to-Peer Distributed Apps," Blockonomi, 3 May 2018. [Online]. Available: https://blockonomi.com/holochain-guide/. [Accessed 2 May 2020].

[69] The MetaCurrency Project, "Holochains for Distributed Data Integrity," The MetaCurrency Project, [Online]. Available: http://ceptr.org/projects/holochain. [Accessed 2 May 2020].

[70] M. Bierling, "Introduction to Holochain, A Post-Blockchain Crypto Technology," Unblock, 16 April 2018. [Online]. Available: https://unblock.net/introduction-holochain/. [Accessed 3 May 2020].

[71] A. Jones, "Exploring Distributed Hash Tables with Beehive," Medium, 26 January 2020. [Online]. Available: https://medium.com/princeton-systems-course/exploring-distributed-hash-tables-with-beehive-1eacd5d78174. [Accessed 2 June 2020].

[72] F. A. Khan, "Chord: Building a DHT (Distributed Hash Table) in Golang," Medium, 11 September 2018. [Online]. Available: https://medium.com/techlog/chord-building-a-dht-distributed-hash-table-in-golang-67c3ce17417b. [Accessed 2 June 2020].

[73] M. Dufel, "Distributed Hash Tables And Why They Are Better Than Blockchain For Exchanging Health Records," Medium, 26 December 2017. [Online]. Available: https://medium.com/@michael.dufel_10220/distributed-hash-tables-and-why-they-are-better-than-blockchain-for-exchanging-health-records-d469534cc2a5. [Accessed 3 May 2020].

[74] Holochain, "Glossary," Holochain, [Online]. Available: https://developer.holochain.org/docs/glossary/. [Accessed 3 May 2020].

[75] Holochain, "04. The DHT: A Public Distributed Database," Holochain, [Online]. Available: https://developer.holochain.org/docs/concepts/4_public_data_on_the_dht/. [Accessed 4 May 2020].

[76] Holochain, "Holochain Core Concepts," Holochain, [Online]. Available: https://developer.holochain.org/docs/concepts/. [Accessed 2 June 2020].

[77] Holochain, "Why Holochain," Holochain, [Online]. Available: https://developer.holochain.org/docs/why-holochain/. [Accessed 3 May 2020].

[78] Holo, "Here's Holochain in 100, 200, and 500 words," Medium, 20 April 2018. [Online]. Available: https://medium.com/h-o-l-o/heres-holochain-in-100-200-and-500-words-509818aa3c88. [Accessed 4 May 2020].

[79] Holochain, "Fully distributed twitter built on holochain," Github, [Online]. Available: https://github.com/holochain/clutter. [Accessed 3 May 2020].

[80] D. Won, "Holochain: The New Blockchain? A Look Beyond the Hype," Hacked, 9 September 2018. [Online]. Available: https://hacked.com/holochain-the-new-blockchain-a-look-beyond-the-hype/. [Accessed 3 May 2020].

[81] C. Turland, "FAQ," Github, 8 Oct Oct 2018. [Online]. Available: https://github.com/holochain/holochain-proto/wiki/FAQ#what-is-holochains-consensus-algorithm. [Accessed 3 May 2020].

[82] N. Zimmermann, "Move over, blockchain: Holochain is coming," 08 11 2018. [Online]. Available: https://www.dw.com/en/move-over-blockchain-holochain-is-coming/a-46203245. [Accessed 4 June 2020].

[83] A. Brock, "Beyond Blockchain: Simple Scalable Cryptocurrencies," Medium, 1 April 2016. [Online]. Available: https://medium.com/holochain/beyond-blockchain-simple-scalable-cryptocurrencies-1eb7aebac6ae. [Accessed 4 May 2020].

[84] D. Atkinson, "Why are Holochain Applications Different and What Does That Mean for Me?," Medium, 4 April 2019. [Online]. Available: https://medium.com/h-o-l-o/why-are-holochain-applications-different-and-what-does-that-mean-for-me-924cd18b6321. [Accessed 4 May 2020].

[85] P. Febrero, "A quick introduction to blockchain scalability," Coinrivet, 10 October 2019. [Online]. Available: https://coinrivet.com/guides/blockchain/an-intro-to-blockchain-scalability/. [Accessed 30 April 2020].

[86] K. Li, "The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed," Hackernoon, 26 January 2019. [Online]. Available: https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44. [Accessed 30 April 2020].

[87] Holochain, "Holo Value Benchmarks," Holochain, [Online]. Available: https://github.com/holochain/benchmarks. [Accessed 4 May 2020].

[88] W. Elcock, "Your Online Data is Stored in These Amazing Places," Guiding Tech, 20 October 2016. [Online]. Available: https://www.guidingtech.com/61832/online-data-stored-amazing-places/. [Accessed 4 May 2020].

[89] B. Marr, "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," Forbes, 21 May 2018. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/. [Accessed 4 May 2020].

[90] Surveillance Self Defence, "A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?," Surveillance Self Defence, 29 11 2018. [Online]. Available: https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work. [Accessed 4 June 2020].

[91] #MetaHash, "What is Blockchain interoperability and why is it important?," Medium, 8 August 2018. [Online]. Available: https://medium.com/metahash/what-is-blockchain-interoperability-and-why-is-it-important-32e4db3bce84. [Accessed 1 May 2020].

[92] S. Cope, "Binary Numbers Explained – Beginners Guide," Steves Internet Guide, 12 May 2019. [Online]. Available: http://www.steves-internet-guide.com/binary-numbers-explained/. [Accessed 27 April 2020].

[93] A. Brock, "https://wiki.p2pfoundation.net/Arthur_Brock_Against_the_Consensus_on_Data_Consensus_in_the_Blockchain," Wiki P2P Foundation, 26 July 2017. [Online]. Available: Arthur Brock Against the Consensus on Data Consensus in the Blockchain. [Accessed 3 May 2020].

[94] Holochain, "Holochain Guidebook," Holochain, [Online]. Available:

https://developer.holochain.org/docs/guide/welcome/. [Accessed 2 June 2020].

10 APPENDIX

10.1 NUMBER SYSTEMS

The decimal number system, which is used in normal life, uses 10 as the base and the numbers range from 0 to 9. When moving from right to left, the value of every number increases with a factor 10. This becomes clear when using the power notation. For example, when representing 105, this becomes the following:

$$105 = 1 \cdot 10^3 + 0 \cdot 10^1 + 5 \cdot 10^0$$

Computer systems however use the binary number system, since transistors can only represent two states, "on" (1) or "off" (0). The binary number system thus uses 2 as the base, instead of 10. The decimal number 105 can be represented in the binary system as follows:

$$1101001 = 1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

The hexadecimal number system uses 16 as the base and the numbers can range from 0 to 15. However, the numbers 10, 11, 12, 13, 14 and 15 are represented as a, b, c, d, e and f respectively. The decimal number 105 can be represented in the hexadecimal system as follows:

$$69 = 6 \cdot 16^1 + 9 \cdot 16^0$$

Numbers on the left thus have a higher value than on the right [92].