Block chain use cases beyond payments

Master’s thesis

[1]

“In cryptocurrency design, computer science & security are far more important than economics & efficiency.” Nick Szabo, computer scientist, cryptographer known for his research in digital currency and smart contracts pioneer

“Blockchains don’t guarantee truth; they just preserve truth and lies from later alteration…” Nick Szabo

Date:	03/11/2017
Study:	Business Administration
Track:	Business Information Management
Author:	Ivan Penkov
Supervisors:	dr. A.B.J.M. Wijnhoven
	dr. C. Amrit

[1] http://www.cryptograffiti.com/

Abstract

Purpose

The purpose of the study is to evaluate block chain technologies for non-monetary use cases, specifically in health care and legal record keeping. The study examines whether the technology can be used beyond censorship-resistant payments using non-monetary transactions. The study compares different block chain types and how they can be applied.

Design/methodology/approach

The study uses qualitative research with semi-structured interviews. Ten experts were interviewed from the fields of health care, legal permits and block chain.

Findings

Health care is not suited for block chain. For the moment, it is unlikely such technology to be used in health care. Unless an ordered data structure is required or there is an ability to use a third party, there is no need for a block chain. Financial services benefit the most from having an ordered data structure. Block chains are still most useful in creating economic values. Legal record keeping and health care would only work with an off-chain trust and a proper identity solution. All use cases apart from value exchange must rely on a third party trust, because the value is already on the block chain in the form of cryptocurrency. Financial services are best suited for block chain for now.

Research limitations/implications

Lack of empirical data because not many use block chains besides payments. Time constraints in expanding the research to DLTs and other block chain based solutions.

Originality/value

The study can be applied to other non-monetary use cases. It is not restricted to only health care and legal record keeping.

Table of Contents

Glossary

API – Application Programming Interface

BGP – Byzantine Generals Problem

Bitcoin – name of a decentralized protocol and a payment network

bitcoin – unit of money on the Bitcoin protocol/network

block chain – continuously growing ordered and time-stamped record of transactions

CGT - Cancer Gene Trust

DLT – Distributed Ledger Technology

ECC – Elliptic Curve Cryptography

ECDSA – Elliptic Curve Digital Signature Algorithm

ether – unit of money on the Ethereum protocol/network

Ethereum – name of a decentralized protocol and a payment network

HIE – Health Information Exchange

ICO – Initial Coin Offering

NDA- Non-Disclosure Agreement

NKI – Nederlands Kanker Instituut (Nederlands Cancer Institute)

P2P – Peer-to-Peer

PoS – Proof of Stake

PoW – Proof of Work

TTP – Trusted Third Party

UCSC – University of California, Santa Cruz

1 Introduction

One of the significant properties and reasons for the existence of block chain is that it empowers a network that is resistant to censorship, meaning transactions cannot be blocked. It is this intrinsic property that makes block chains interesting. What Nakamoto (2008a) introduced to the world is truly unique and disruptive. He wrote a paper in 2008 called "Bitcoin: A Peer-to-Peer Electronic Cash System," introducing a new digital currency based on cryptography, and later the following year in 2009 he released the first implementation. To manage the currency, he also introduced the block chain which is a data structure for recording transactions allowing people to transact without the need of a central authority or administration and without the need to know one another (Wilson, 2017a, p. 4). Bitcoin is a technology for financial sovereignty, not controlled by any government or institution. A popular use case for a cryptocurrency like Bitcoin is to speculate on its price (new users buy coins hoping for more new users to do the same so that the price would go up). At first, there were no services or products to be bought with bitcoins, so demand for buying coins was mainly speculative. Later, Bitcoin became used as a currency on the darknet markets (online markets for illegal goods). Its usage as a currency on those markets created a non-speculative demand because customers were buying the currency to circumvent the regulatory restrictions of buying the illegal goods. It makes the trade of illicit goods possible with small interference from the law (Christin, 2012, p. 2). One of the most popular darknet markets was the Silk Road marketplace which was shut down by the FBI in 2013 (Wikipedia, 2017h). Because of its pseudonymous and hard to track nature Bitcoin makes services like the Silk Road flourish. It also helped with the funding of Wikileaks (Greenberg, 2011) when their bank accounts were seized by the authorities (The BBC, 2010). In general, Bitcoin is useful for paying for anything that would be otherwise censored by the traditional system. According to Sztorc (2017) the reasons to use Bitcoin for payments can be:

- *"legal reasons (online drug sales, ransomware payments, tax evasion, gambling, hiding assets)*
- *privacy reasons (pornography, HIV-test)*

- *technical reasons (i.e., "smart contracts" such as multisig, pay-for-data*[2]*, pay-for-document*[3]*, pay-for-wifi"* ("The two types," para. 3)

The popularity of digital currencies in recent years has led to a significant shift away from the crypto-anarchist communities towards the communities of professional investors, financial experts, law firms, and even banks (Tasca, 2015, p. 29). In a recent joint report from Coinbase and ARK Invest it was estimated 54% of Coinbase users use bitcoin strictly as an investment (Burniske & White, 2017, p. 8). Even though the Bitcoin scene is transforming into a tamer arena where people are building applications and services that make use of the block chain, and venture capital is invested in potentially serving a common good, one should always keep in mind whether there is a real need for such technology in specific use cases. Traditional systems can solve most problems with higher efficiency.

The block chain space is flooded with scams and short-lived projects. Those projects issue digital tokens to distribute to people before offering an actual product in exchange for investments. Most of the projects exist to capitalize on the speculative nature of individuals who invest in projects with the hope they could become wealthier. Those individuals believe that those new tokens could become as valuable as the bitcoins are. Usually, those startups purposely try to imitate Bitcoin so they can sell their tokens easier. Many early adopters in Bitcoin became wealthy and are looking for ways to invest their money into new venues. There will be a time when funds will dry up and investing will slow down. It is essential to be aware of such vulnerabilities as this is still highly unregulated space.

This study evaluates a technological aspect of Bitcoin called the block chain and why companies would have a particular interest in this technology for non-monetary use cases. The study starts with an analysis of the block chain in chapter 2; it presents some background information on the creation of Bitcoin, marking the first generation of block chains, some technical analysis and how it evolved. Then, different use cases are discussed in chapter 3 and their application in a public and private sector. Next, an analysis of the views and opinions of interviewed experts is presented in chapter 4, and finally, the study ends with a conclusion and discussion in chapter 5. For the rest of the introductory chapter 1, the

[2] Paying for verification of identities stored on a block chain (Sztorc, 2016).

[3] Decentralized way for paying for leaked sensitive information in trustless manner by encrypting the information and selling the decrypt key. Also it can be used for paying for files: "proprietary software, open source software, corporate documents, firmware drivers, movies" (Todd, 2014).

motivation, the scope, and the objectives of the study together with its methodology and research plan are discussed.

1.1 Motivation for the study

Block chains are attractive because they offer a new working solution to an old computer science problem for distributed networks, which is discussed in sub-section 1.1.2 “Byzantine Generals Problem.” The motivation of the study is to evaluate the technology in use cases beyond payments, with a special focus on health care and legal record keeping (certificates, titles, permits). In reality, no one wants to use a block chain unless he or she has to. There are many block chain projects with a lot of hype and extraordinary claims. The study tries to point where block chains can be handy as some use cases can turn to be “vaporware[4].” The study is motivated by a paper of Wüst & Gervais (2017) “*Do you need a Blockchain?*” There are many potential block chain use cases apart from payments. In fact, some of the claims encompass all areas of life, for example, tracking of tuna (Peters, 2016), and providing firefighters with unlimited communication channels (Cheliak, 2016).

Block chains are designed to remove the need for a central administration (Wilson, 2017a, p. 8), and that makes them interesting for research in health care, where the administration is a big necessity and trust is of intrinsic value. It is interesting to investigate how identities are managed by the block chain for the case of health care. Legal record keeping is interesting use case because there are already some companies that experiment with block chain. There is also a public organization “Het Kadaster” from the Netherlands that created a block chain prototype. It is interesting to investigate whether block chains can be used as a source of truth for proof of ownership for the case of legal records.

Permissionless and permissioned block chains are useful for different purposes. Permissionless block chains are proven useful, for now, for creating economic incentives and money. Permissioned block chains aim at creating more efficient consensus protocols, to be used in business operations.

There is a lot of marketing and hype on block chain technologies. There were 1.6 billion dollars invested in block chain startups since 2014 (see **Figure 1**). Things are in a bubble, so this study will try to filter out the marketing from the content in block chain and show where

[4] “Software or hardware that has been advertised but is not yet available to buy, either because it is only a concept or because it is still being written or designed” (Oxford Dictionaries, 2017).

this technology would make sense to be applied. “ICOs[5] have surpassed angel and seed-stage funding for all internet companies since the beginning of the summer” (see **Figure 2**) (Williams-Grut, 2017). The money from those investments can go so far without a use case. Eventually, the money will allocate to utility and shift away from the space if there are no use cases.

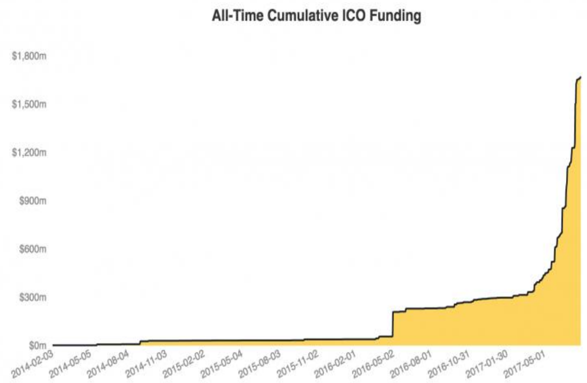


Figure 1: *ICO funding for block chain startups (Tian, 2017)*

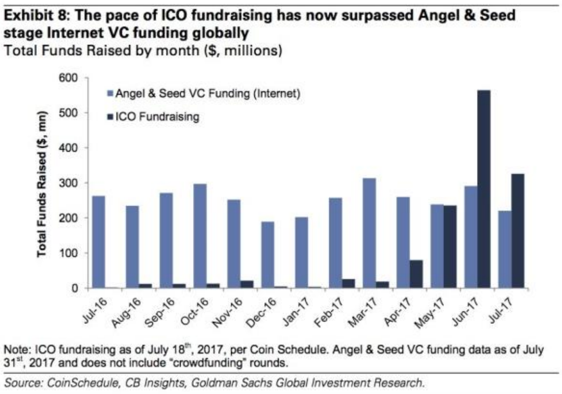


Exhibit 8: The pace of ICO fundraising has now surpassed Angel & Seed stage Internet VC funding globally
Total Funds Raised by month ($, millions)

Note: ICO fundraising as of July 18th, 2017, per Coin Schedule. Angel & Seed VC funding data as of July 31st, 2017 and does not include "crowdfunding" rounds.

Source: CoinSchedule, CB Insights, Goldman Sachs Global Investment Research.

Figure 2: *Total funds raised by source of financing (Williams-Grut, 2017)*

The excessive block chain hype on projects which are not yet ready can harm because probably there are much more efficient solutions already in existence which can do a better job. Most of the hype is generated to sell tokenized block chain projects where the incentives are to increase the value of the token itself (Tierion, 2016, p. 5).

1.1.1 Disruptive technology

Block chain disrupts mainly the traditional middlemen model (Schneider et al., 2016, p. 3). The block chain is a “publicly reviewable ledger where every transaction is recorded and verified without the need of a trusted intermediary” (Giaglis & Kypriotaki, 2014, p. 6). For example, it would help reduce the need for bank intermediaries because it offers security, easy access, fast settlement and transparency of data (Schneider et al., 2016, p. 69). By removing intermediation layers of financial inclusion, it gives direct control over financial activities (Ciaian, Rajcaniova, & Kancs, 2016, p. 917). As with any disruptive innovation, this technology could create new industries and potentially new markets. For example, mining pools (a way of collectively mine bitcoins) are emerging, also, new payment systems, privacy-oriented services and payment anonymization (Giaglis & Kypriotaki, 2014, p. 8).

[5] “Developers, businesses, and individuals increasingly are using initial coin offerings, also called ICOs or token sales, to raise capital” (Investor.gov, 2017).

There are even claims that the disruptive innovation of block chain has not only the potential to change Finance, but also to change people's daily life through non-financial applications (notaries, smart contracts. music, storage, internet applications, IoT) (Nofer, Gomber, Hinz, & Schiereck, 2017, p. 185). Wilson (2016a) states that "block chain is almost universally labeled as disruptive, but it's really too early to tell" (p. 3). One of the most significant contributions of block chain could be the birth of new generations of Distributed Ledger Technologies (DLT) (Wilson, 2016a, p. 3). For financial institutions, the disruption can come in the form of improved business processes, and operations as distributed ledger and similar consensus technologies are becoming an interest for them (Wilson, 2016a, p. 14).

Yee (2014) discusses where the value of Bitcoin lies. He states that it is not about becoming a substitute for money, but instead becoming the "Internet of Money" (p.3). Bitcoin is much more than a replacement - it is like a "logical layer for finance" (Yee, 2014, p. 2). See **Figure 12** in section 2.2 for an explanation of the layers of the internet and how block chain fits that model. Choucri & Clark (2012) describe the logical layer as a layer that contains the internet protocols such as TCP/IP (the communication language that makes the internet work) (p. 3). The TCP/IP protocol allows for anyone to develop applications on top because no permission is necessary (Yee, 2014, p. 3). The same is valid for the Bitcoin protocol. It could be used for programming applications for finance and other areas on top.

The Bitcoin protocol controls all transaction, so people can program money to come with conditions. "For instance, money will be released only if a third person agrees, or people will fund a project only when a threshold is passed" (Yee, 2014, p. 3).

Bitcoin is open source, meaning the software source code is available for anyone to study, change, and distribute for any purpose (Laurent, 2004, p. 4). It is also declared to be backed by math because it uses public-key cryptography, specifically Elliptic Curve Cryptography (ECC) which facilitates the creation of public keys through elliptic curve multiplication (Antonopoulos, 2014, p. 62). The Elliptic Curve Digital Signature Algorithm (ECDSA) is a signature generation and verification algorithm in ECC, which is required in Bitcoin for sending transactions to others and for verifying that the sender is the authentic owner of the funds. The ECDSA is a U.S. government standard that has gone through cryptographic analysis over the years, so it is believed to be very secure (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016, p. 40). Elliptic curves are explained in sub-section 2.3.3 . Such cryptographic functions are hard to reverse. They are easy to calculate in one direction and impractical to calculate in the opposite direction (Antonopoulos, 2014, p. 62). The math behind the strength of the private keys in Bitcoin is explained in sub-section 2.3.1 . Such math proofs are irrefutable, and math has trust embedded into it (Bradbury, 2013, p. 5), which is why some believe Bitcoin can manage a monetary system. Andreas Antonopoulos, one of the most prominent figures in Bitcoin, even claimed that this technology shifts the model of trust from people to math (Antonopoulos, 2014). Trusting math-money only makes sense to the extent that the block chain is only used without human intervention. However, the performance of the block chain still depends on human decisions. Furthermore, in the case when real-world assets become represented on a block chain, human intervention becomes necessary to register those assets to the holders (Wilson, 2016a, p. 8).

A generalization on what Bitcoin and block chain solve, Patterson (2015) summarizes in four questions:

1. *"How do you update everybody's ledger at the same time without a "master" ledger?*
2. *How do you prevent fraudulent transactions?*
3. *What happens if two ledgers ever disagree with each other?*
4. *How do you prevent changes being made after-the-fact[6]?" (p. 8)*

In sub-section 1.1.4 it is revealed how the protocol solves those four questions.

1.1.2 Byzantine Generals Problem

Lamport, Shostak, & Pease (1982) introduced the Byzantine Generals Problem (BGP), in a paper titled "The Byzantine Generals Problem." The problem is a thought experiment for reaching an agreement in a distributed systems with possible components that give false information to other parts of the system. "A reliable computer system must be able to cope with the failure of one or more of its components" (Lamport, Shostak, & Pease, 1982, p. 382).

In computer networks, different conflicts can arise from requests to a server (Rijnbout, 2017, p. 41). The problem of conflict requests in a computer system is abstractly comparable to that of a group of Byzantine generals trying to coordinate an attack together (Lamport et al., 1982, p. 382).

The strategy exercise describes how several generals surround a hostile country. All generals have different divisions that camp in separate valleys outside the hostile country. The

[6]"Occurring, done, or made after something has happened after-the-fact approval an after-the-fact review" (Merriam-Webster, n.d.-a)

generals must reach an agreement to “attack” or “retreat” simultaneously by communicating with one another through their lieutenants. Some of the subordinates might be traitors (potentially even the generals) who spread false information to the rest (Lamport et al., 1982, p. 383). Traitors are dangerous because they can undermine processes.

The situation creates issues for which the generals must have an algorithm that guarantees two conditions:

A. “All loyal generals decide upon the same plan of action” (Lamport et al., 1982, p. 383).

“The algorithm must guarantee condition A regardless of what the traitors do” (Lamport et al., 1982, p. 383). The loyal generals will do what the algorithm says they should, but the traitors may do anything they wish. Additionally, the loyal generals, apart from reaching an agreement, must also agree on a reasonable plan (Lamport et al., 1982, p. 383):

B. “A small number of traitors cannot cause the loyal generals to adopt a bad plan” (Lamport et al., 1982, p. 383).

Condition B needs a definition of what a bad plan is. Information gathered by the generals from monitoring the enemy is analyzed, and each general decides for the best plan of action and votes for that plan. The final decision can be based on a majority vote (Lamport et al., 1982, p. 383). To achieve condition A, all loyal generals decide upon the same plan of action, by using the same method of information combination. To achieve condition B, a small number of traitors cannot cause the loyal generals to adopt a “bad plan,” by using a robust method (based on a majority vote) (Lamport et al., 1982, p. 383). “A small number of traitors can affect the decision only if the loyal generals were almost equally divided between the two possibilities, in which case neither decision could be called bad” (Lamport et al., 1982, p. 383).

Generals communicate their values $v(i)$ (the information communicated by the ith general) to one another. Traitorous generals may send false values to generals. Therefore, the following must be true for condition A to be satisfied:

1. “Every loyal general must obtain the same information $v(1),\ldots, v(n)$” (Lamport et al., 1982, p. 383).

Traitor *i* may send different values of *v*(*i*) to various generals, so generals who obtained *v*(*i*) directly from the *i*th general cannot be directly trusted. For every *i* (whether or not the *i*th general is loyal) condition 1 becomes:

1'. “Any two loyal generals use the same value of v(*i*)” (Lamport et al., 1982, p. 384).

A situation where generals receive values "retreat,"..., "retreat" when every loyal general sent the value "attack" should not happen. Therefore a new condition is required for each *i*:

2. “If the *i*th general is loyal, then the value that he sends must be used by every loyal general as the value of *v*(*i*)” (Lamport et al., 1982, p. 383).

Conditions 1' and 2 are about the way the *i*th general sends a single value. The problem can be summarized to how a commanding general sends his value to his lieutenants. Specifically, a commanding general must send an order to his (*n* – 1) lieutenant generals (*n* is the number of generals) such that the Interactive Consistency conditions (IC) hold (Lamport et al., 1982, p. 384):

IC1. “All loyal lieutenants obey the same order” (Lamport et al., 1982, p. 384).

IC2. “If the commanding general is loyal, then every loyal lieutenant obeys the order he sends” (Lamport et al., 1982, p. 384).

1.1.3 Impossibility of results in the BGP

Generals can send only oral messages. An oral message is one whose contents are entirely under the control of the sender so that a traitorous sender can send any message (Lamport et al., 1982, p. 384). A solution to the BGP will only work if more than two-thirds of the generals are loyal. For example, if there is a single traitor among three generals, then there is no solution to the problem (Lamport et al., 1982, p. 384).

See the example of **Figure 3.** From the perspective of L1, he receives *v*(1) = attack and *v*(2) = retreat. Following IC2: L1 must obey the order of the commander (attack); IC1: L1 needs to obey the same order as L2 (retreat). In this example, it is not obvious for L1 whether L2 is the traitor.

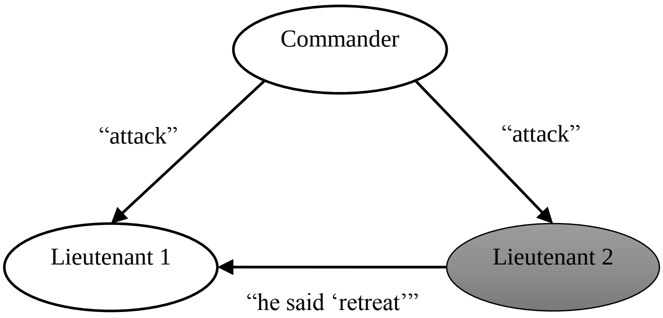


***Figure 3:** Lieutenant 2 is a traitor* (Lamport, Shostak, & Pease, 1982, p. 385)

In the next scenario (see **Figure 4**), it is also not apparent for L1 whether L2 is a traitor. L1 does not know what message the commander sent to L2 and L2 does not know what message the commander sent to L1. From the perspective of L1, both examples appear the same (he receives two different orders). “If the traitor lies consistently, then there is no way for L1 to distinguish between these two situations” (Lamport et al., 1982, p. 384). From the point of view of L2, it is evident that he can receive any message from the commander (attack or retreat), so he cannot know whether the commander is lying.

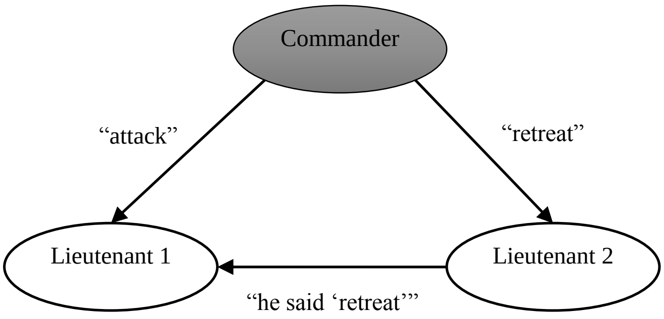


***Figure 4:** The commander is a traitor (Lamport et al., 1982, p. 385)*

L1 and L2 must obey the order from the commander in both situations because of IC2. However, in **Figure 4** their decisions violate IC1 because both obey different orders (Lamport et al., 1982, p. 385). The results of Lamport et al. (1982) “show that no solution with fewer than (3*m* + 1) generals can cope with *m* traitors” (p. 385). Solving the problem with messages requires (3*m* + 1) or more generals. Lamport et al. (1982) explain that in detail in “3. A solution with oral message” (p. 387) and “4. A solution with signed messages” (p.

390). However, this is not of interest for this study, and in the next sub-section 1.1.4, the research explains a solution with “proof of work” in Bitcoin.

1.1.4 Restating the BGP problem in Bitcoin

The BGP can be summarized as a decision-making problem in which multiple actors participate. Each participant is uncertain about the information they receive. Therefore they need to verify each other’s information.

The Bitcoin network applies a Byzantine consensus protocol (Miller & LaViola, 2014, p. 1). Nakamoto (2008b) explains the BGP in a rephrased setting where the generals want to attack the King’s Wi-Fi password. The generals communicate through a network, and after they crack the password, they must erase all logs to hide the attack. They need to attack in a short time to avoid detection, and each general does not control enough CPU power to attack alone. Therefore, they need to attack at the same time. The proposed time of the attack can come from a traitor trying to sabotage the plan, but that does not matter because there are no bad plans in the problem outline. The problem is that when many generals send out a time of the attack at the same time, the other generals might receive the messages in a different order because the network is not instantaneous (Rijnbout, 2017, p. 42).

Therefore, using the requirements of the classic BGP it follows:

1. “All processes in the network must come to unanimous agreement about some value, in spite of a minority of faulty processes that deviate arbitrarily from the protocol” (Miller & LaViola, 2014, p. 1)

Requirement 1 means that not all generals must find the same value (date and time) since it is not specified how many generals (how much CPU power) are needed for the attack (Rijnbout, 2017, p. 42). Therefore, the algorithm needs another requirement:

2. “The generals are able to check whether they have enough combined CPU power to execute a successful attack at the proposed time of attack” (Rijnbout, 2017, p. 42).

The two requirements Nakamoto (2008b) states can be satisfied using a voting system called Proof of Work (PoW), which is similar to the voting scheme utilized in the classic BGP version. According to Miller & LaViola (2014) “Bitcoin is based on a novel Byzantine consensus protocol” (p. 1). In the case of Bitcoin, the messages of the generals are the transactions that peers send to one another. The problem narrows down to what is the order of transactions, which transactions come first and whether the previous owner in a transaction sent any earlier transactions from the same set of coins (Nakamoto, 2008a, p. 2). The network solves this problem in a decentralized manner without a trusted party. Nodes publicly announce every transaction to the network, check if the output of a transaction has been previously spent and agree on the validity of which transaction came first (Nakamoto, 2008a, p. 3). Because the system is not instantaneous, finding which transaction came first is a problem. Therefore, transactions are time-stamped by inclusion in a PoW block[7] "to generate computational proof of the chronological order of transactions" (Nakamoto, 2008a, p. 1). The time-stamping proof is the answer to Patterson's (2015) question "*How do you prevent fraudulent transactions?"*

There is a subset of nodes called "miners." Their function is adding new blocks to the block chain, as long as those blocks are in line with the consensus rules. Also, miners compete with one another (Narayanan et al., 2016, p. 69). Each miner works on solving a cryptographic puzzle to satisfy the PoW condition. The solution results in a SHA-256 hash of all data included in a block (Nakamoto, 2008a, p. 3). A solution is found every ten minutes, so the block chain does not grow in space too big too fast (Nakamoto, 2008a, p. 4). Each new hash includes all new transactions, the previous block hash, the new time-stamp and the new nonce (Nakamoto, 2008a, p. 3). "To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes" (Nakamoto, 2008a, p. 3).

PoW makes the network resilient to Byzantine attacks, to an extent. An attack where the attacker modifies a block will only be successful if his chain becomes longer (with more significant PoW effort) than the "honest" chain and the majority of computing power switches to the attacker's chain (Nakamoto, 2008a, p. 3). For example, each subsequent block after b_1 will be b_2, b_3 , b_4 , …, b_n. If an attacker wants to falsify transaction *t* in b_1, he will need to do more and more work with each newly added block b_n to the honest chain. The probability of a successful attack decreases with each block after *t* (Rijnbout, 2017, p. 43). Nakamoto (2008a) calculates using probability theory that "as the number of blocks the attacker has to catch up with increases" (p. 7) the chance of him catching up decreases

[7] Blocks contain permanently recorded transactions (Bitcoin Wiki, 2016b).

exponentially. This problem is explained as the double spend attack (spending the same coins more than once in more than one transaction) (Rijnbout, 2017, p. 43).

> *"Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. An attacker can only try to change one of his own transactions to take back money he recently spent" (Nakamoto, 2008a, p. 6).*

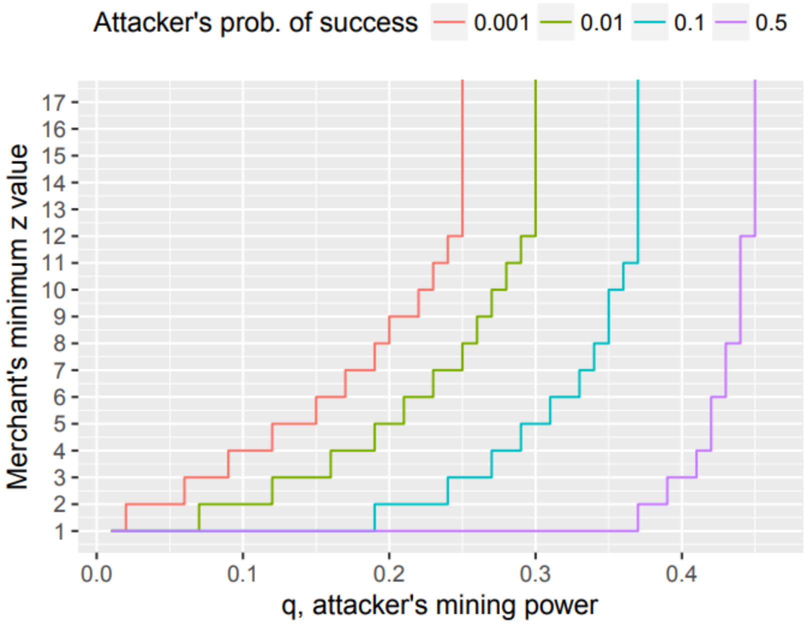


Figure 5: *Attacker probability of success in double spending (Ozisik & Levine, 2017, p. 11)*

Figure 5 shows the likelihood of a successful attack in relation to mining power and confirmed blocks[8] (*z* value). It is based on an improved model of Nakamoto's (2008a) calculation formula on the probability of a successful attack (p. 6). Ozisik & Levine (2017) point out some of the errors in Nakamoto's formula and also determine which components of his model are not perfect (p. 1). **Figure 5** shows that the more mining power someone has, the higher the probability of a successful attack, therefore, the more minimum confirmations *z* a merchant should accept. For example, given an attacker's mining power of 0.2 and a desired probability of success of less than 0.001, the plot shows a minimum required confirmations of 10. The PoW algorithm, even though its resistance against double spend attacks is based on probability, answers Patterson's (2015) question *"How do you prevent changes being made after-the-fact?"*

[8] When a user broadcasts a transaction to the network, it awaits to be included in a block. When that happens, the transaction gets mined at a depth of one block. Each newly mined block, after the block that includes the initial transaction, increases the number of blocks deep by one. Prevention against double-spending usually requires a transaction to pass minimum six confirmations (six blocks) (Bitcoin Wiki, 2017a).

The PoW also answeres another of Patterson's (2015) question “*How do you update everybody’s ledger at the same time without a “master” ledger?”* The PoW is a mechanism for archiving consensus about the order of transactions without a central ledger (Rijnbout, 2017, p. 43). In a more simplified model of Bitcoin’s PoW, someone can imagine it as a tool for reaching consensus among the generals in the BGP. In this case, each general has to work on a relatively hard problem, so that it would take, on average, ten minutes to solve, if all generals work at the same time. Once a general finds the solution to the problem (the time of the attack of King’s Wi-Fi), he sends it to the rest of the network and all other generals update their version of the problem to include the time of the attack. The generals continue working on the next PoW problem and thus creating additional subsequent solutions which are chained together all the way to the first one. The generals working on a different plan will always switch to the longest available chain, as it is the chain with the most CPU power (Rijnbout, 2017, p. 44). Following the longest chain is what answers Patterson's (2015) question “*What happens if two ledgers ever disagree with each other?”*

It should take one hour for completing six solutions and chaining them together if all participants work on the same chain. It also means that they are working on the same version of the plan when to attack King’s Wi-Fi. If the chain reached six solutions in one hour, then it means the majority of the generals worked on the same plan of attack. Therefore, they can proceed safely with attacking at the scheduled time included in the chain (Rijnbout, 2017, p. 44).

The consensus protocol of Bitcoin does not need a trusted party. In the traditional BGP solutions, there is always a central authority (the Commander). Apart from consensus the Bitcoin protocol also gives an estimate on the success of an attack (necessary confirmations). It also could prevent from duplicate plans sent at similar times and thus lower the risks of sabotaging attempts (double spending) (Rijnbout, 2017, p. 44).

A general rule for Bitcoin transactions to be safe is to wait for six confirmations. Accepting instant transactions (with zero confirmations) is not considered safe. Karame, Androulaki, & Capkun (2012) show by experimenting, how double spend attacks can succeed “with overwhelming probability,” and “do not incur any significant overhead on the attacker” (p. 13). They experimented with attacks in fast payments, where the time between sending and receiving is few seconds (Karame et al., 2012, p. 1). Naturally, attacks can still happen, and the generals in the BGP are not concerned with receiving false plans. In the classic BGP, it is enough just to have a consensus even if it is false as long as the majority agrees. The PoW gives a consensus of the majority. However, this consensus also has to agree on the validity and honesty of transactions to have a secure payment network (Rijnbout, 2017, p. 44).

1.2 Scope of the study

The field of Information Systems (IS) has been slower in the process of realizing the potential of digital cryptocurrencies, even though they are considered a breakthrough in finance, economics, and computer science. Those currencies can create trustless decentralized monetary systems not controlled by governments or central banks. Lawmakers are crafting new public policies and laws on regulating this technological phenomenon, and yet research on cryptocurrencies in a scientific field like IS is somewhat scarce. There are some established forums, like the First Workshop on Digital Currencies (DC2014), held in conjunction with the International Conference on Business Information Systems but the general outlook is not very dense regarding research (Giaglis & Kypriotaki, 2014, p. 4).

This study tries to contribute with research on the topic of cryptocurrencies. It focuses in detail on Bitcoin’s block chain, because it is by far the most secure public storage of value. It is the first and the most trusted block chain in existence. The maximum coins will only be 21 million, and a user can transfer value across borders in near real time. Bitcoin’s block chain has the most prominent network effect, the highest hash rate (hence the most security) and some of the smartest cryptographers are working on the code base, including Adam Back (the creator of the PoW used in Bitcoin and cited in Nakamoto’s paper). Most of the papers and research in this study are based on Bitcoin. At the moment around 80% of block chain research is on Bitcoin and 20% on other block chains (Yli-Huumo, Ko, Choi, Park, & Smolander, 2016). When there is a reference to “the block chain” it is meant Bitcoin’s block chain unless specified otherwise. Other types of block chain and alternatives to block chain are examined as well.

The examined period includes recent events and some notable critical events from the past which are relevant to the topic. Some of the research was hard to obtain through the usual channels for publishing because block chains are still not very popular in academia. Luckily, Bitcoin has a big community where one can find help in obtaining specific research materials. For example, Reddit, Twitter, Telegram, and YouTube were good ways to connect with people of interest. Reaching out to Christopher DeRose from Bitcoin Uncensored on YouTube assisted in contacting Stephen Wilson who provided two of his reports on block chain for this research.

Some of the limitations of the study are concerned with the lack of available data. Block chain Research Lab from the University of Hamburg stated in an email exchange that “empirical work is hard to gain access to.” There is no available data for analysis, or it is not accessible to the public. Additionally, most companies doing block chain projects are not public, or they sign non-disclosure agreements (NDAs) with their software vendors. Another limitation is that block chains are hard to understand. It seems that it is a complicated subject even for experts in the field (Bitcoin Uncensored, 2017, 35:25). Nowadays, the term block chain is subject to many interpretations, and it is diverting from its original meaning defined by Nakamoto in the Bitcoin source code. Recently, Elaine Ou from Bloomberg said, “...the term ‘block chain’ has been so misappropriated that no one knows what it means anymore” (Ou, 2016).

1.3 Objectives

The objective of the study is to evaluate block chain in the context of security, trust, ownership, and provenance. Block chain is useful, thus far, for censorship-resistant payments. The study expands this notion and examines whether block chains can be used beyond value transfers by means of non-monetary transactions. The study examines what is accomplished by using a block chain and compares similar solutions with one another, and how a real organization could implement such technology.

1.4 Research methodology and research plan

The study uses semi-structured interviews for undergoing a qualitative research. It uses inductive reasoning to build up a general conclusion based on evaluating specific presented facts and analyzing collected data. Analysis on block chains would potentially help others see where it can be most useful. There is interest in block chains. The research design aims at assessing the accomplishments of this new technological phenomena.

The research design will serve the purpose of answering the following research question:

“What are the probable outcomes for block chain implementation in health care and legal record keeping?”

Qualitative research is appropriate because there is not much data on block chains in the world. However, there is available literature even though still limited but enough to analyze the research question. The theory is concrete enough to make an analysis, so there is no need to create a new theory. There is no specific methodological rule set for conducting qualitative research. The value of the research methods depends on the specific setting of the study, and the actual consequences of the research strategy (Maxwell, 2009, p. 233).

The interview questions generate data that is needed to understand the matter identified by the research question (Maxwell, 2009, p. 230). Semi-structured interviews were carried out with a diverse group of experts from the block chain space (vendors, computer scientists, and critics) and specialists from the industries of interest (notary and health care).

The interview questions are relatively similar for all participants, especially the opening questions. However, the follow-up questions differ according to the area of expertise of the individuals, to explore the views of each interviewee towards the topic. During the interview process, the study was explained together with its objectives. The interviews are designed to account for the foundation of the research and subsequently introduce the specifics of the subject. Each interview starts with introducing the main research question and the purpose of the interview. Then, it continues with specific topic questions. Most of the interviews start with asking the participants what their interpretation of a block chain is. Then, during the follow-up questions if there was a necessity for clarification, probing questions were asked. The interviews end with a closing question usually asking the participants to speculate on the future of block chains in health care, legal records, and other non-monetary uses.

The interviews were conducted in the comfort of the interviewees at a time suitable for them. Due to significant distances as some of the participants are from different continents, interviews were conducted via video or email. Others were conducted in person or via phone. The interviews were in English.

Semi-structured interviews combined with literature analysis allows for a complete view of the context of block chains, health care, and legal records and brings reliable contact with the field because it allows for gathering data from the inside. However, multiple interpretations are possible with qualitative research because there are no standardized methods for measuring the results. The collected data is used to undergo an analysis and contribute to the conclusion.

2 Analysis of block chain

The following chapter focuses on how block chains work and how they have progressed since the inception of Bitcoin. The first generation of block chains have a similar structure to Bitcoin. Thus, Bitcoin is used for the technical examples in this chapter. In section 2.1, there is some background information about how Bitcoin was started, and the attributes of the different block chain types. All the layers of the Bitcoin’s block chain are found in section 2.2, and in section 2.3 is the math that makes block chains work. In the last section 2.4, there is a description and presentation of what transactions are.

2.1 Background of Bitcoin and block chain

The idea of decentralized electronic cash is not new, and researchers imagined it for a long time. At that time they found out that it was not possible to implement a decentralized model with peer-to-peer nodes which would not necessarily know or trust one another without a trusted third party (TTP). Moreover, this misses the desired decentralization aspect (Giaglis & Kypriotaki, 2014, p. 5).

Nearly all of the exciting ideas and technologies in Bitcoin (distributed ledgers, BGP) can be traced back twenty years ago (Narayanan & Clark, 2017, p. 23). For example, time-stamping, proof of work and Merkle trees originated by Haber and Stornetta, Dwork and Naor and Ralph Merkle respectively, are technological components that can be found in the academic literature of the 1980s and ’90s (Narayanan & Clark, 2017, p. 1). Nakamoto’s talent was to put together the underlying technologies in a specific way, which could explain why Bitcoin took so long to be invented (Narayanan & Clark, 2017, p. 3).

Bitcoin is the first trustless payment system and digital store of value. Even though some defined block chain as “a machine for creating trust” (the Economist, 2015, p. 13), this is not entirely true, and this study shows why. Bitcoin is the name of protocol and currency (bitcoin, BTC, XBT). The protocol represents a revolutionary development, with disruptive potential in computer science, cryptography, and distributed systems (Giaglis & Kypriotaki, 2014, p. 4). Bitcoin is the first public decentralized network with a public ledger of transactions, reaching a consensus through PoW (Bastiaan, 2015).

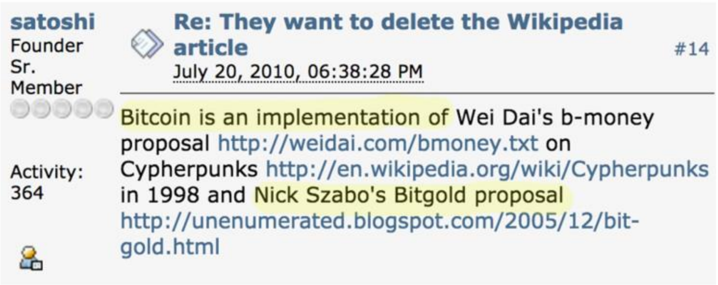
Users often see Bitcoin as an example of a digital bearer asset. Bearer assets are similar to cash. The person holding the asset is the only one who can spend it, without a bank or a third party. According to Investopedia (2017), ‘Bearer Instrument' are securities where no ownership information is recorded. The holder is presumed to be the owner, and whoever is in possession of a physical bearer bond is entitled to the coupon payments (Investopedia, 2017). For a first time in history, there is a digital equivalent of a bearer asset. Through the virtues of cryptography and the block chain, it is possible to prove digital asset ownership and also to authorize ownership transfers. “Ownership of an asset is determined by the knowledge of a private key” (BitFury Group, 2016, p. 8). A private key proves a claim to balance on the block chain. Cryptocurrencies like bitcoin are not IOUs or credit instruments. Owners can digitally sign transactions with their private keys to transfer bitcoins to other people (Wilson, 2016a, p. 4). The exchange of balances is recorded on the block chain. Users do not own bitcoins, they own the private keys to balances, and the coins are ethereal, lacking material substance (Wilson, 2016a, p. 5).

Block chain as a concept can be traced back to the works of Stuart Haber and W. Scott Stornetta in 1991, who discuss a cryptographically secured chain of blocks. Later publications followed, and in 2000 Stefan Konst published a general theory for cryptographically secured chains and suggestions how to implement. Even though there were publications, none of them were applied in any way.

Nick Szabo has come close enough to the concept of Bitcoin with his project in 1998 of decentralized digital currency that he called “bit gold” (Wikipedia, 2017e). The mechanism which he designed was never implemented (Wikipedia, 2017f, “Bit gold”). However, his bit gold idea was using similar to Bitcoin mechanism of PoW, time-stamps, digital signatures, and double-spent prevention via a Byzantine-resilient peer-to-peer method, which was discovered that unlike Bitcoin it was vulnerable to attacks (Bitcoin Wiki, 2016a). Nick Szabo is called to be "a direct precursor to the Bitcoin architecture," and some even speculate he was the anonymous creator of Bitcoin.

> *“A researcher by the name of Skye Grey believes the real Nakamoto is* ***Nick Szabo****. For one, Szabo developed a system called “bit gold”, which is a direct precursor to the Bitcoin architecture. People have also taken into consideration an analysis of Szabo’s writing style and his cool reaction to Bitcoin given that he’d spent nearly ten years working on cryptocurrencies. Szabo denied being Nakamoto. The evidence linking this “origin story” to Bitcoin’s creation is interesting but hardly convincing.” (O’Leary, 2016, “Three Possible Candidates,” para. 1)*

Furthermore, in a forum post on the bitcointalk.org forum, Nakamoto called Bitcoin "an implementation of Nick Szabo's Bitgold proposal."



satoshi
Founder
Sr.
Member

Activity:
364

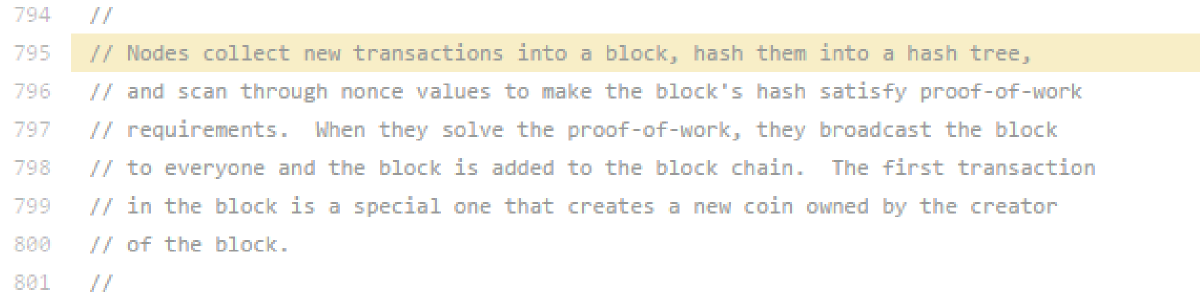
Re: They want to delete the Wikipedia article
July 20, 2010, 06:38:28 PM
#14

Bitcoin is an implementation of Wei Dai's b-money proposal http://weidai.com/bmoney.txt on Cypherpunks http://en.wikipedia.org/wiki/Cypherpunks in 1998 and Nick Szabo's Bitgold proposal http://unenumerated.blogspot.com/2005/12/bit-gold.html

Figure 6: *Bitcoin and bit gold relation (satoshi, 2010, post #14)*

One of the reasons why Szabo thinks it took so long for Bitcoin to emerge after bit gold is that the bit gold/Bitcoin ideas were very far from obvious for most people, and people did not know much or read about bit gold (Szabo, 2011). Szabo (2011) tells that Nakamoto improved a significant security weakness in his design, and managed to reduce the threat of faulty parties taking control of the majority of nodes which could spread conflicts in the network. The solution was the requirement of PoW to be a node in the Byzantine Fault Tolerant peer-to-peer system (Szabo, 2011).

Nakamoto's definition of "block chain," cannot be found in his paper. In fact, there is no mentioning of the word anywhere in his paper. However, the definition is found in the source code of the first release of the protocol "BitCoin v0.01 ALPHA," in "main.h," starting at line 795 (see **Figure 7**). Sections 2.2 and 2.4 cover some of the mechanisms from **Figure 7** in detail.



```
794  //
795  // Nodes collect new transactions into a block, hash them into a hash tree,
796  // and scan through nonce values to make the block's hash satisfy proof-of-work
797  // requirements.  When they solve the proof-of-work, they broadcast the block
798  // to everyone and the block is added to the block chain.  The first transaction
799  // in the block is a special one that creates a new coin owned by the creator
800  // of the block.
801  //
```

Figure 7: *Definition of a block chain by Nakamoto (livegnik, 2016)*

2.1.1 Block chain attributes and goals

There are two types of block chain – permissionless and permissioned (Wüst & Gervais, 2017, p. 6). Both are sometimes referred to as Distributed Ledger Technologies (DLTs) (Wilson, 2017a, p. 4).

Permissionless block chains operate in untrusted environments encouraging open innovation. Permissioned block chains encourage authorized innovation and allow a small number of people to run nodes similar to a centralized database. Nodes are blocked for the public to participate (Wüst & Gervais, 2017, p. 1). There is also a hybrid type which allows the public to monitor the chain but does not permit the public to write on the chain.

Permissionless block chains are Bitcoin and Ethereum. They are open and decentralized. Anyone can join the network and run a node. Developers can develop software and use the open source materials without asking a central body for membership. Everything is open, and anyone can see and read the ledger without being banned and without the need for registration (Wüst & Gervais, 2017, p. 1).

Permissionless block chains are claimed to be incorruptible. According to the Merriam-Webster dictionary, "incorruptible" can be defined as:

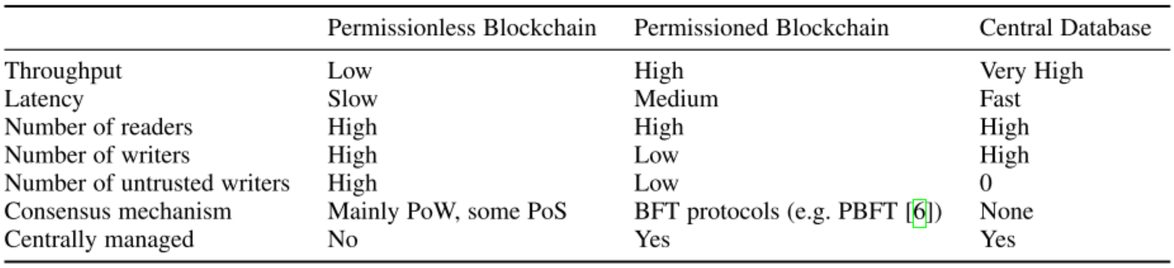
> *"Incapable of corruption: such as*
>
> *A: not subject to decay or dissolution*
>
> *B: incapable of being bribed or morally corrupted"* (Merriam-Webster, n.d.-b)

Data is transparent on permissionless block chains, it cannot be removed from the network and cannot be corrupted because altering information or overriding the entire network would require the total amount of the computing power used to produce the current state of the chain. However, corrupting the network is possible in theory, but practically it is unlikely to happen because the network is public and others will take notice of the attack. If someone takes control and captures Bitcoin, it will be noticed by the public, and that would affect the value of the currency, which will decline rapidly making it impossible for the attacker to exchange bitcoins for real money.

A weakness for permissioned block chains is the computing power constraints due to reduced participation in the network (fewer peers) (Krawiec et al., 2016, p. 9). Permissioned block chains only allow selected readers and writers. There is a limit on the number of peers that can join. They are attractive for their accelerated processing time of transactions (Krawiec et al., 2016, p. 8). There is a central authority which decides who can join, similar to a membership model. Some models allow writers and readers also to run separated parallel block chains that are interconnected. Some of the most well-known permissioned block chains are Hyperledger Fabric and R3 Corda (Wüst & Gervais, 2017, p. 2).

Table 1 differentiates the properties of the different block chain types and a central database. It is interesting to note how centralized databases have better throughput and latency than block chains. The additional complexities that block chains add because of their consensus mechanisms affect their performance negatively. The transaction throughput of Bitcoin is seven transactions per second (tps) which can potentially attain an effective increase of throughput above sixty tps without compromising the security of the system (Gervais et al., 2016, p. 4). In comparison, VISA is capable of processing more than fifty thousand tps (Visa, 2015). Throughput comes at the expense of decentralization. This tradeoff is essential to consider when making decisions on block chain use (Wüst & Gervais, 2017, p. 2).

Table 1: *Permissionless, permissioned block chains and centralized database (Wüst & Gervais, 2017, p. 3)*



	Permissionless Blockchain	Permissioned Blockchain	Central Database
Throughput	Low	High	Very High
Latency	Slow	Medium	Fast
Number of readers	High	High	High
Number of writers	High	Low	High
Number of untrusted writers	High	Low	0
Consensus mechanism	Mainly PoW, some PoS	BFT protocols (e.g. PBFT [6])	None
Centrally managed	No	Yes	Yes

2.1.2 Costs

Permissioned block chains' operational costs are unknown (Krawiec et al., 2016, p. 8). However, a report from Santander InnoVentures estimated that block chain technologies could be saving the banks annually $20B in costs by 2022 (Perez, 2015). Such estimate shows that an investment of $200M to pay for the block chain enterprise experiments in R3 (Williams-Grut, 2016) is not significant and could be justified by cost savings. R3 is a consortium working on implementing permissioned block chain technology in the financial services and "has recently completed a successful transfer of commercial paper between banks" (Higgins, 2016). The open source properties of block chains and the distributed nature of the technology can help reduce the cost of operations. The costs to transact on the network derive from the volume and size of transactions submitted through the network. Furthermore, the type of transactions on the chain (data storage, smart contracts, value exchange) dictates the costs (Krawiec et al., 2016, p. 9). The cost saving from transactions and the increased security could save billions of dollars for governments and prominent organizations. However, block chain experiments still need to demonstrate a long-term transformational value (Krawiec et al., 2016, p. 10). There are not many block chains in the world to make a forecast about possible costs of operating at scale, especially for permissioned block chains (Krawiec et al., 2016, p. 9).

2.1.3 Implementation

Implementation of a block chain comes down to choosing a permissionless (e.g., Bitcoin, Ethereum), or permissioned block chain (e.g., MultiChain, R3 Corda, Hyperledger Fabric, Microsoft's Blockchain as a Service). There are examples where Ethereum is also used for permissioned block chains. It is a platform that claims to allow the creation of decentralized applications on top of a block chain architecture (Krawiec et al., 2016, p. 3). Permissionless block chains have access to more computing power and allow for broader acceptance and open innovation which makes them an appealing choice. However, Bitcoin and Ethereum are constrained by maximum transaction volume (Krawiec et al., 2016, p. 8). Processing of transactions in permissioned block chains is faster and could be incentivized financially or by exchange for access to a particular block chain data (Krawiec et al., 2016, p. 8). Deciding whether to use permissionless or permissioned block chains, one should consider what information needs to be stored on or off the block chain (Krawiec et al., 2016, p. 8).

Choosing a block chain can be structured in a flowchart in **Figure 8.** Block chain can be seen as a form of database (Wüst & Gervais, 2017, p. 2). If no storing of data is required, then block chain is unnecessary. If there is more than one party involved in changing the state of the database, a block chain will provide additional guarantees than a regular database (Wüst & Gervais, 2017, p. 2). If there is an always online TTP, then there is no need for a block chain because all write and verify operations can be delegated to the TTP. If the TTP is offline or not present, it can function in the setting of a permissioned block chain, where all writers are known (Wüst & Gervais, 2017, p. 2). If all writers trust one another, a database with shared write access is an ideal solution (e.g., Google Sheets). If the opposite is true, where writers do not trust one another, and they are known, a permissioned block chain is suitable (Wüst & Gervais, 2017, p. 2). Public verifiability means that anyone is allowed to read the permissioned block chain. If that is not mandated, then a private permissioned block chain is a solution (Wüst & Gervais, 2017, p. 2).

If the multiple writers are unknown, a permissionless block chain is a suitable to use. It only makes sense to use it when "multiple mutually mistrusting entities want to interact and change the state of a system" without a third party (Wüst & Gervais, 2017, p. 2). To use any block chain boils down to whether the operation is unable to use a TTP.

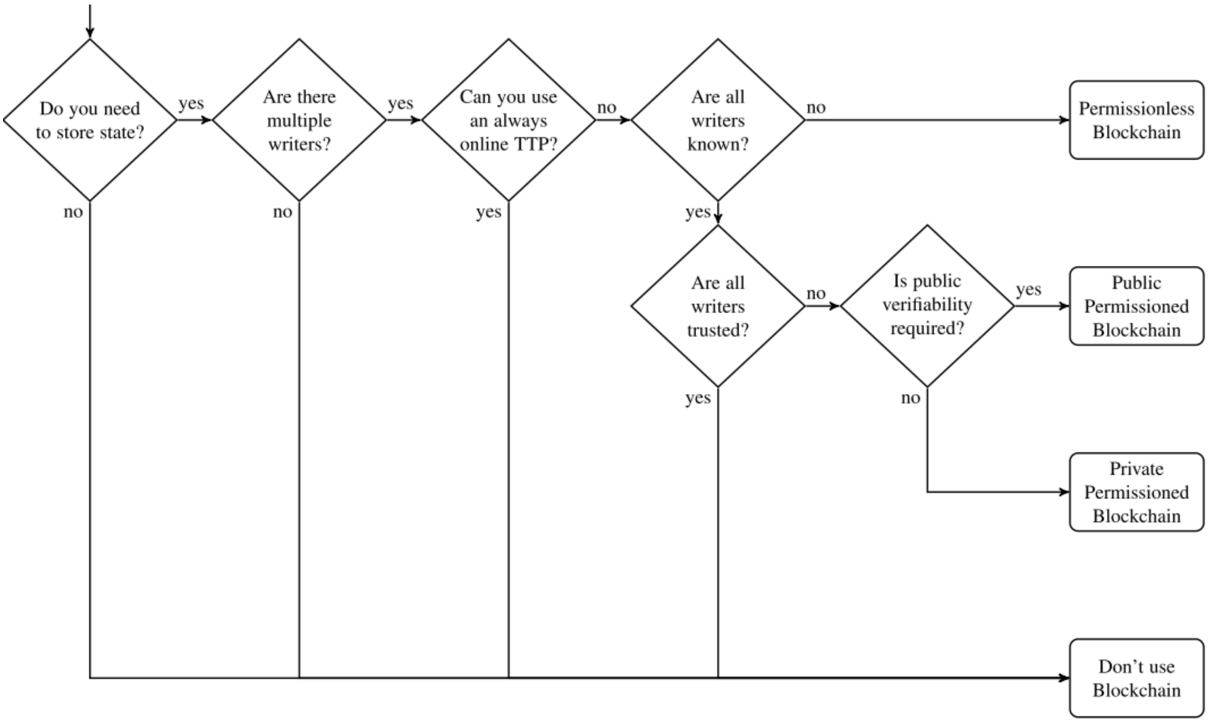

Do you need to store state?
yes
no
Are there multiple writers?
yes
no
Can you use an always online TTP?
no
yes
Are all writers known?
no
yes
Permissionless Blockchain
Are all writers trusted?
no
yes
Is public verifiability required?
yes
no
Public Permissioned Blockchain
Private Permissioned Blockchain
Don't use Blockchain

Figure 8: *Block chain flow chart (Wüst & Gervais, 2017, p. 3)*

2.1.4 Block chain laws and regulations in various countries

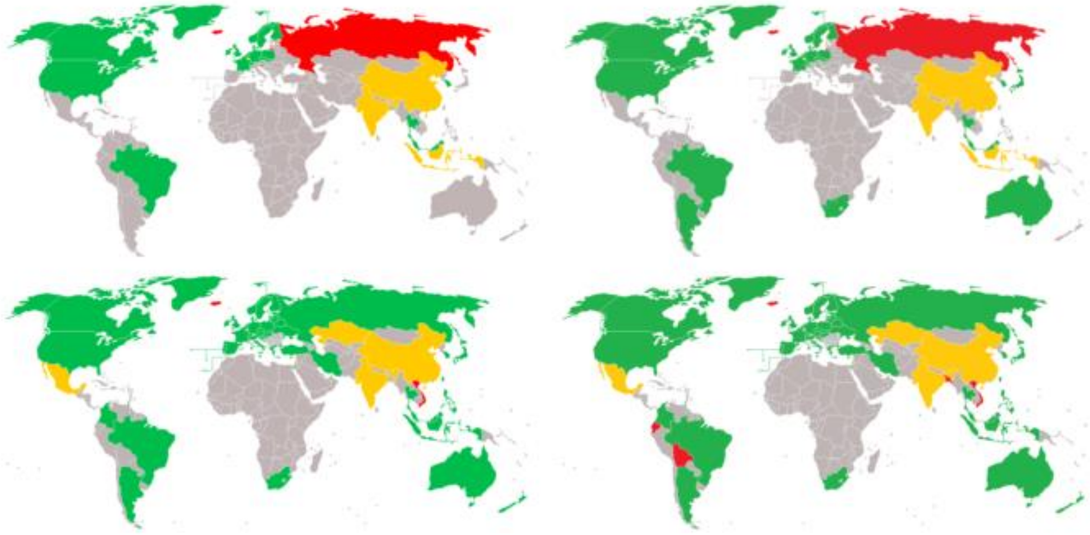


Figure 9: *Status of digital currencies (Tasca, 2015, p. 27)*

Figure 9 shows the legal status of digital currencies in different countries. "From left to right and top to bottom - February, March, April, September of 2014" (Tasca, 2015, p. 27). Green: permissive countries, red: hostile countries, Yellow: contentions countries, grey: unknown position (Tasca, 2015, p. 27; BitLegal, 2017). Russia has a habit of banning and permitting cryptocurrencies, adapting all positions contemporaneously which shows how unclear the legal situation still is. As of recently, Russia is once again not Bitcoin-friendly with banning Bitcoin-related websites (O'Leary, 2017).

De Nederlandsche Bank started a project in 2015 to map the developments in the scope of innovative finance: examining implications on payments, credit intermediation, investment and insurance and others. DNB uses an analysis to map how different sectors could develop from using this technology to optimize the regulatory environment (Tasca, 2015, p. 42).

In a short interview, DNB answered that they cannot speculate on the future outcomes of the technology. However, they do acknowledge the technology's potential. Their current position is that virtual currencies, such as bitcoin, fall outside the scope of the Financial Supervision Act (Wet op het financieel toezicht - Wft), which means that they do not supervise virtual currencies or enterprises trading or facilitating payments in these. This is not to say, however, that the Wft offers no foothold to bring virtual currencies or the trade or payment in these under official supervision. Such a development could happen in the future. Further information that they provide regarding the technology can be read from their annual report (De Nederlandsche Bank N.V., 2016, pp. 84-86). They describe the technology as promising, but it needs more research. They are particularly interested in the currency side and what it holds for payments than anything else.

2.2 Block chain

The following section discusses the block chain and its layers. To give more clarity as to how Bitcoin is positioned in the world **Figure 10** shows an onion representation. The intersection at the top can be seen as a means to skip layers. For example, PoW can be used to burn electricity to produce heat. So there is an indirect consequence that is connected to other sectors without needing to go through layers (Möser, Böhme, & Breuker, 2014, p. 18). The onion also shows how one can exit Bitcoin directly at the intersect via peer-to-peer cash exchange, or via the financial system (bank wires) through the onion layers.

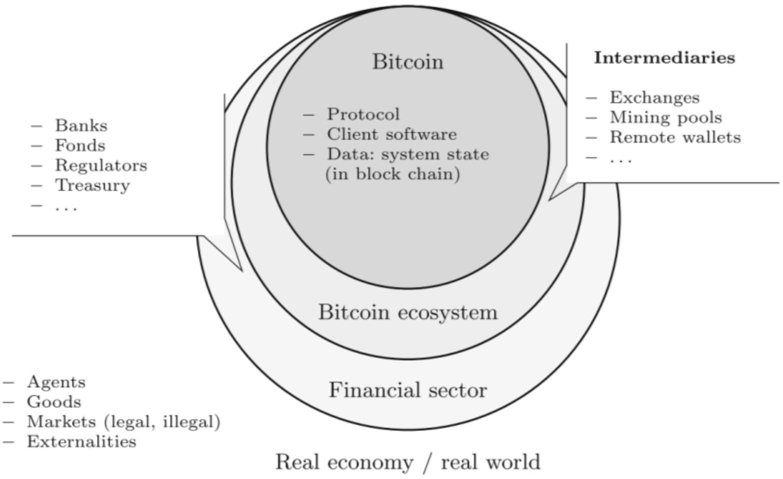


Figure 10: *Bitcoin's relation to the world* (Möser, Böhme, & Breuker, 2014, p. 18)

Next, this section presents a model of the block chain application stack in relation to the layers comprising the internet. It shows how the block chain fits the internet layers introduced by Choucri & Clark (2012). There are two models – OSI (Open Systems Interconnection) network model and TCP/IP (Transmission Control Protocol and the Internet Protocol). Both models are different – OSI is seven-layered standard, and TCP/IP is a four-layered standard, and both standards are well established and used in network architectures as a guideline for communication applications. **Figure 11** compares the TCP/IP and OSI network models.

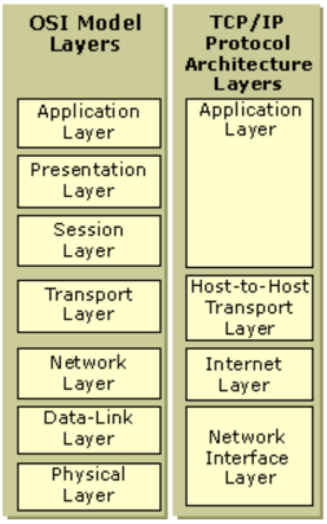


Figure 11: *Comparison between seven-layer OSI and four layer TCP/IP models (Microsoft, 2017)*

For this research, the model of the internet layers of Choucri & Clark (2012) will be used which is similar to the TCP/IP network model but simpler. The application stack of Bitcoin is inspired by Monegro, Wilson, Wenger, & Ali (2014), and transformed by using ArchiMate software for the architecture modeling and modified by adding layer (layer 2) of technologies that were not present in the original model (see **Figure 12**).

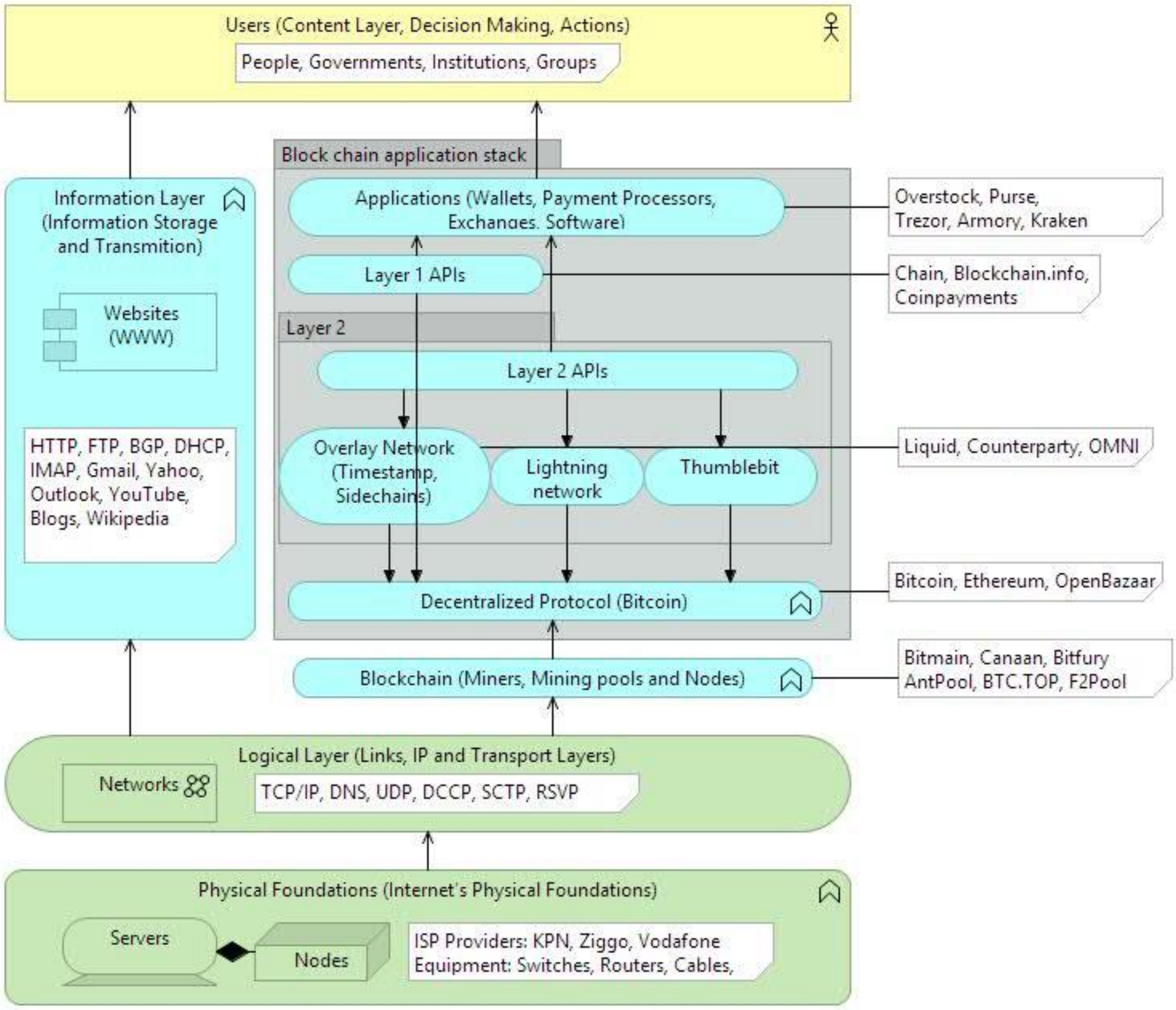

Users (Content Layer, Decision Making, Actions)
People, Governments, Institutions, Groups
Block chain application stack
Information Layer (Information Storage and Transmition)
Websites (WWW)
HTTP, FTP, BGP, DHCP, IMAP, Gmail, Yahoo, Outlook, YouTube, Blogs, Wikipedia
Applications (Wallets, Payment Processors, Exchanges, Software)
Overstock, Purse, Trezor, Armory, Kraken
Layer 1 APIs
Chain, Blockchain.info, Coinpayments
Layer 2
Layer 2 APIs
Overlay Network (Timestamp, Sidechains)
Lightning network
Thumblebit
Liquid, Counterparty, OMNI
Decentralized Protocol (Bitcoin)
Bitcoin, Ethereum, OpenBazaar
Blockchain (Miners, Mining pools and Nodes)
Bitmain, Canaan, Bitfury AntPool, BTC.TOP, F2Pool
Logical Layer (Links, IP and Transport Layers)
Networks
TCP/IP, DNS, UDP, DCCP, SCTP, RSVP
Physical Foundations (Internet's Physical Foundations)
Servers
Nodes
ISP Providers: KPN, Ziggo, Vodafone
Equipment: Switches, Routers, Cables,

Figure 12: *The internet layers (Choucri & Clark, 2012) and the Bitcoin's application stack (Monegro et al., 2014) (own conceptualization)*

The block chain application stack is built vertically bottom up in a similar fashion as the internet. The upper layers depend on the bottom and not the other way around. Solum & Chung (2004) thought of the cyberspace as a model consisting of six layers, which later Choucri & Clark (2012) formalized into a more straightforward model composed of four layers:

- *"The physical foundations – the Internet's bricks-and-mortar, from fiber-optic cables to cell towers, personal computers, and servers.*

- *The logical layer –the Internet protocols, World Wide Web, browsers, domain-naming system, websites and software that make use of the physical foundations.*
- *The information layer –the encoded text, photos, videos, and other material that is stored, transmitted, and transformed in cyberspace.*
- *The users – the people and constituencies who shape the cyber-experience and the nature of cyberspace itself, by communicating, working with information, making decisions and carrying out plans" (Choucri & Clark, 2012, p. 2).*

It is important to note that no one has designed Bitcoin yet or block chain in a layered approach similar to the internet's (Torpey, 2016, para. 1). Bitcoin is still work in progress, so additional layers are being built with time. At the moment, with two layers already in existence, if there were a block chain based internet, it would look like the conceptual example in **Figure 13**. The block chain would serve as a base layer if a decentralized internet were to be built on top. Other layers can use the block chain for anchoring data, transactions, or data for domain names.

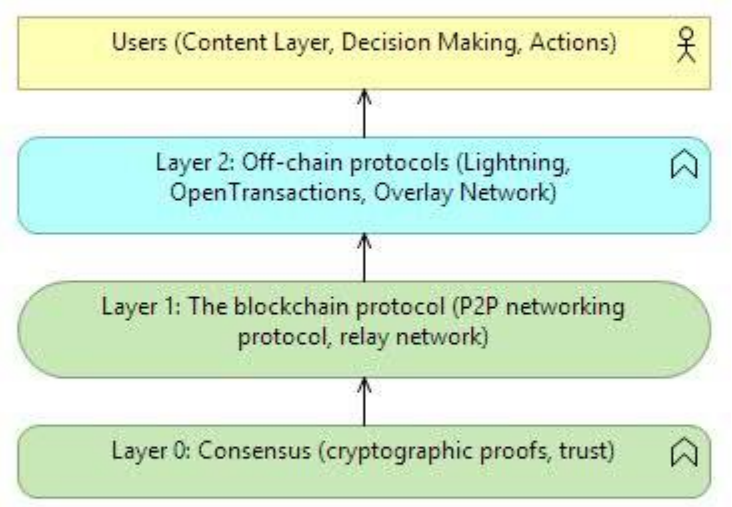

Users (Content Layer, Decision Making, Actions)
Layer 2: Off-chain protocols (Lightning, OpenTransactions, Overlay Network)
Layer 1: The blockchain protocol (P2P networking protocol, relay network)
Layer 0: Consensus (cryptographic proofs, trust)

Figure 13: *Block chain layers (own model)*

2.2.1 Layer 0: Consensus

Miners and the nodes compose the block chain which is mostly a network of computers working together to verify all Bitcoin transactions. Bitcoin uses TCP to propagate transactions and blocks on the network (Antonopoulos, 2014, p. 144). The algorithm incentivizes miners by rewarding them with bitcoins. The miners record transactions in blocks on the block chain and the nodes verify whether the newly mined blocks are valid.

After validation, miners can claim the block reward for their work (Antonopoulos, 2014, p. 202).

The most prominent companies in 2017 offering mining equipment are Bitmain, Canaan, and Bitfury. Those companies specialize in Application-specific Integrated Circuit (ASIC) hardware, which is customized for particularly mining Bitcoin or another cryptocurrency.

Bitcoin miners behave strategically and form pools. To lower the variance of rewards, pools help distribute at infrequent intervals rewards according to the shares each miner has. (Eyal & Sirer, 2014). The difficulty of a single miner finding a block is increasing with time because of competition. Pools help miners distribute rewards equality among one another according to their contributions. Multiple miners contribute to the generation of a block. Thus the rewards get split. Two of the ASIC manufacturers also own pools – AntPool (Bitmain) Bitfury (Bitfury). **Figure 14** is a pie chart of the distribution of mining power in different pools.

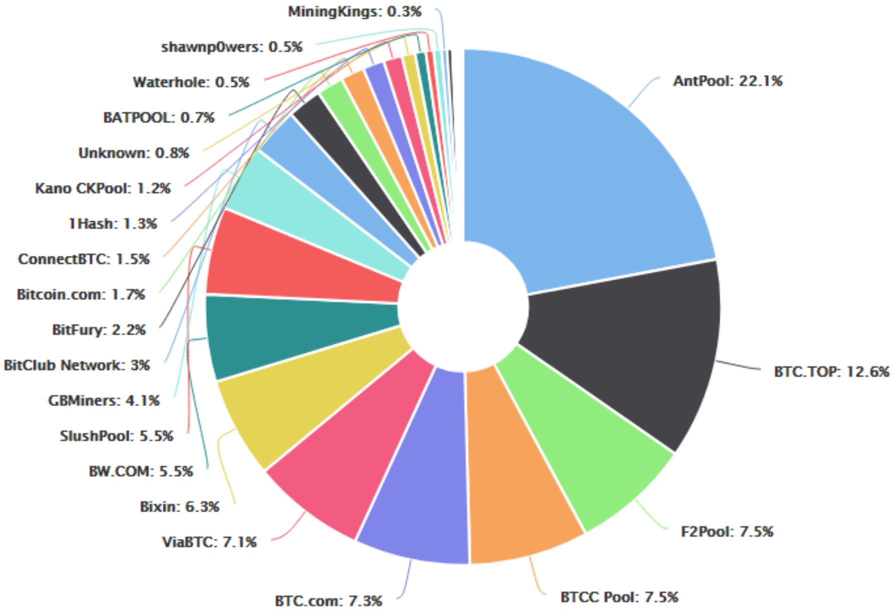


Figure 14: *Bitcoin mining pools (Blockchain.info, 2017)*

Miners are also the producers of the digital asset. The chances of a miner solving the puzzle first depend on his mining power (hardware resources). His chances increase with increased mining power. “This reward structure provides an incentive for miners to contribute their resources to the system and is essential to the currency’s decentralized nature” (Eyal & Sirer, 2014).

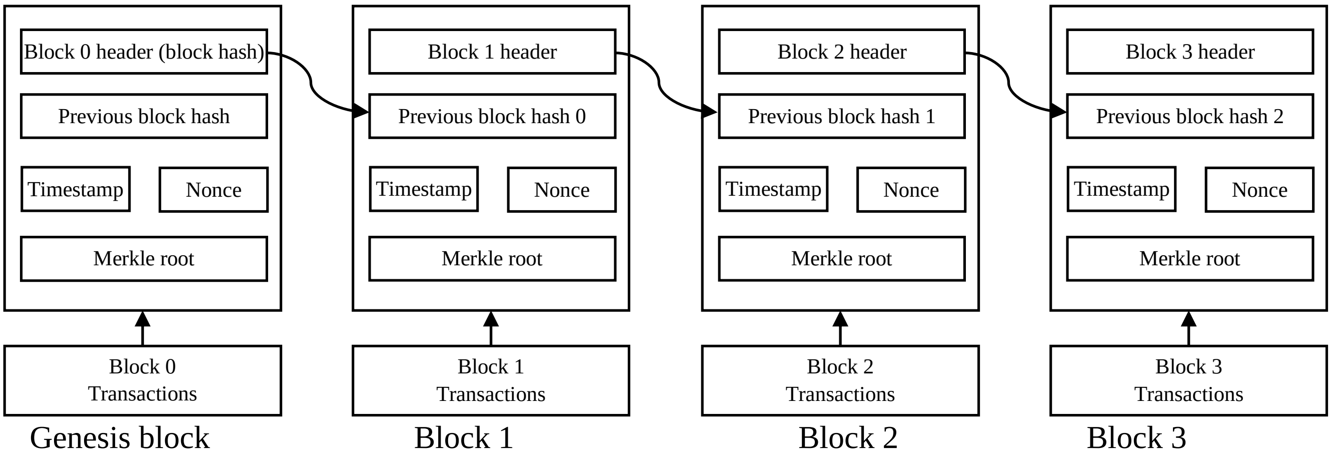


***Figure 15:** Simplified example of a block chain (Nofer et al., 2017, p.184) (own modification)*

The blocks are "chained" by the hashes and thus become a block chain (Nofer et al., 2017, p.184) (see **Figure 15**). Every new block includes the hash of the previous, thus creating a chain of blocks. A nonce is a meaningless random number for verifying the hash. The purpose of adding this number is to create unpredictability and uniqueness of the data (European Union Agency for Network and Information Security (ENISA), 2016, p. 31). The reward or block reward is a form of subsidy given to miners for finding a block. This reward is included in the "coinbase transaction" which is the first transaction of each block. The amount of the coinbase is equal to all the fees from all transactions in a block plus the subsidy. Through this additional subsidy (the reward) is how the network creates new coins. The creation of new coins decreases by half every four years.

Hashing is a one-way cryptographic function, which means that it cannot be reversed. It compresses data to a tiny size. In contrast, a typical encryption process is reversible (decryption), and usually encrypted data becomes larger than its decrypted state. A hash only serves the purpose of verifying if, for example, data is unmodified, but it cannot decrypt the data, it is impossible to calculate the input from the hash. A hash is similar to what a fingerprint is. A hash is unique for every data. If one thing is changed in the data, the hash also changes.

Example data and their hashes:

This is a piece of text! — 34f79yw587w94r7q0243ry057yrw935fw5hk
This is a piece of text. — fodjxc98syfxeos4ifs3847rt9q34arfleuh (Versteegh, 2014, "Hash")

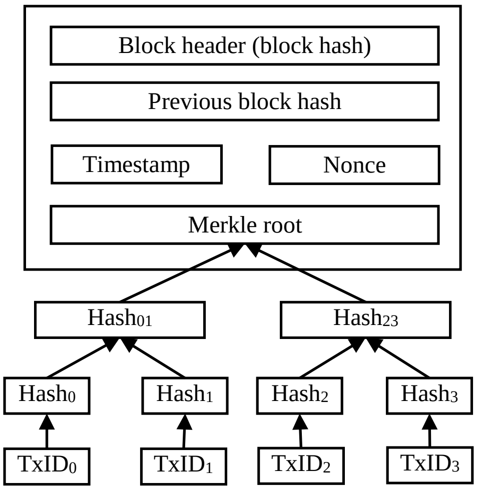


Figure 16: *Merkle tree (Tschorsch & Scheuermann, 2016, p. 2102)*

Figure 16 shows how the Merkle tree integrates a Merkle root into a block (Tschorsch & Scheuermann, 2016, p. 2102). It is also known as a hash tree. Merkle tree can expand infinitely. All transactions are hashed before they are included in a block. Then all hashed results are paired and hashed again until a single hash remains – the Merkle root (Tschorsch & Scheuermann, 2016, p. 2102). All blocks headers must include the Merkle root of a Merkle tree of all transactions in a block. Clients can verify if the particular transaction is part of a block by "traversing the branches up to the root" (Tschorsch & Scheuermann, 2016, p. 2102).

Ralph Merkle (1989) invented the Merkle trees (or "Digital signature system and method based on a conventional encryption function") and filed for a patent. Merkle trees are essential for a block chain. In 2009 the patent expired, hence the increase of block chain projects in recent years. There is not much publicity around this little-known fact. Nowadays, as the patent is expired, anyone can implement Merkle trees and start a block chain.

Merkle tree which is also called binary hash tree can make a large piece of data minimal, allowing quick access for referencing and provability (Merkle, 1990, pp. 218, 229). If someone has specific data, he or she can prove ownership by the hash. The hash is the proof. Another patent for the Merkle trees is "Method of providing digital signatures" (Merkle, 1982). Section 2.3 explains digital signatures in Bitcoin in detail.

> *"The invention comprises a method of providing a digital signature for purposes of authentication of a message, which utilizes an authentication tree function of a one-way function of a secret number" (Merkle, 1982, "Abstract").*

The technologies used in block chains can be entirely novel and secure. Block chain could be seen as a safe place to store information and money, but that also comes with some risks.

Bitcoin's decentralized network is in danger of constant attacks. It was attacked in the past and will be attacked in the future. Some of the challenges with securing the network are examined by Bradbury (2013), who also cites Sergio Lerner, a cryptography expert who suggests paying security researchers to review each new patch in the code of Bitcoin as a necessity to ensure the code stays secure and stable (p. 8). Additionally, at any time there could be an attack such as the malicious forks of Bitcoin from August and November 2017, which lead to confirm an earlier discovery of potential coup attempt to monopolize Bitcoin and centralize its mining power to one entity (Peck, 2015).

A fork may be generated temporarily in the block chain because many miners almost simultaneously succeed in the PoW. In such a case, the longer chain is the authentic one. Therefore, to finalize a transaction, it is necessary to confirm that the relevant block chain does not fork after miners incorporate the transaction data into a block. After that, miners create multiple blocks, and the chain continues. When miners create approximately additional six blocks, then that chain becomes relevant and authentic (see **Figure 17**) (Nomura Research Institute, 2015, p. 11).

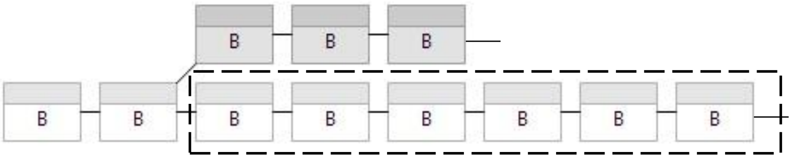


Figure 17: *Hard fork (own model)*

The longer chain is considered the authentic chain in the event of a hard fork. To make a false transaction, it is necessary to continue creating blocks faster than the authentic fork (Nomura Research Institute, 2015, p. 11). Mining past blocks to alter a past state of the block chain requires a “50% or a larger percentage of the machine power (computing capacity) of all computers participating in PoW” (Nomura Research Institute, 2015, p. 11). Forks can be viewed as a consensus failure. One chain is saying one truth, and the other is saying another.

Proof of work (PoW)

PoW is a system where mining structures burn electricity to create security for the coins so that no one can create extra coins (capped at 21 million bitcoins) or double spend. There is an actual competition to generate new coins. Participants need to burn much electricity and buy mining equipment to create new coins and validate transactions. A participant would buy dedicated computing power to solve cryptographic puzzles. Miners include each solution to the next challenge. This process creates a growing chain which continually changes its properties. The majority of participants have to agree (reach BGP consensus) on the new solutions to begin the next puzzle. This process of mining is required to prevent the double spending problem and to secure the network so that reproduction of data twice is forbidden. The PoW is unique for block chains, and it makes them immutable. It is the only known way to have an immutable public network where anyone can have write permission to the data structure. The prevention of double spending is what makes PoW a superior BGP consensus.

A new block that contains the correct hash is found by miners every ten minutes (Nakamoto, 2008a, p. 4). The goal of the ten minute block time is to avoid forks and to make sure everyone is on the same chain and to give time for the miners to define what is the longest chain. Also, there are people with slow internet connections on the planet, for which the network needs to account. The ten minute period increases the security of the network, and it also disallows the block chain to grow too much too fast (Nakamoto, 2008a, p. 4).

Miners maintain the network because of the incentive structure of the system which gives rewards in bitcoins (BTC or XBT, the unit of the network) for each newly generated block. The idea of adding new coins into circulation gets its inspiration from gold mining, where miners expand their operation to find new gold. In the case of Bitcoin, instead of expanding territory to find new gold, it is CPU power and time that is expanding (Nakamoto, 2008a, p. 4). There will be a time when all coins will be in circulation so that supply of new coins will stop and the mining incentive will be placed entirely on transaction fees. Transaction fees are voluntary. The sender can assign any fee value or no fee at all. However, if the fee is low or nonexistent, it can create a disincentive for miners to accept the transaction into the next block. The fee is an incentive for the user to have their transaction included in the next block. Otherwise, they will have to wait longer times for processing until a miner accepts. Logically, if the network is growing more users join, so transaction volume increases, which results in higher fees because there is greater competition among users. Users are willing to pay higher fees than others so that miners can process their transactions with priority. One of the assumptions is that in the future when the miners create all coins there will already be enough users on the network that a subsidy will no longer be necessary, and fees will be sufficient to cover the expense for electricity to mine blocks (see **Figure 18**).

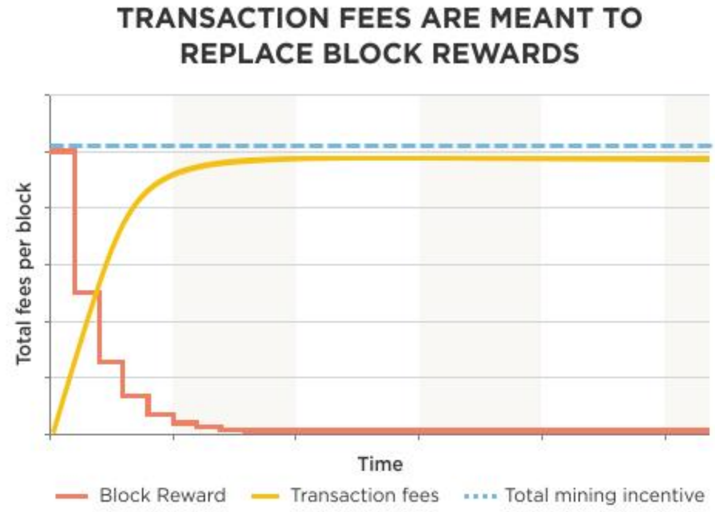


Figure 18: *Transaction fees and block rewards (Bitsonblocks, 2016, "Why do miners mine?")*

Proof of Stake (PoS)

In PoS, there are special nodes called "validators" which are voting on valid blocks (ENISA, 2016, p. 10). Unlike PoW where users invest in computing power, PoS relies on the users to prove the authenticity of the network by holding a stake in the network, by holding the token (ENISA, 2016, p. 10). Therefore, the process is not called mining but rather it is called "staking" which is a form of "virtual mining." Anyone with a stake can be a validator on the network. Voting happens when coins are locked as a deposit until a network reaches consensus. "The next valid block is the one which has the majority of deposits (at least 51%) allocated to it" (ENISA, 2016, p. 34). The system forfeits deposits of validators who try to iterate the voting process by suddenly switching the vote to a different block (ENISA, 2016, p. 34). In PoS it is possible to process more transactions per second than in PoW (ENISA, 2016, p. 34).

In PoS by holding the coins participants earn more coins, similar to interest. If a million coins get created, they are distributed to people who want to purchase them. PoS block chains can be seen as permissioned because participants need to purchase the tokens to stake (mine). Whereas in PoW participants still need to purchase mining hardware or they can make their own if they can. PoW allows referencing "truth" outside of the system through energy expenditure. PoS is a closed system favoring the token holders. PoS is less secure and still experimental.

2.2.2 Layer 1: The block chain protocol

Nodes on the network communicate with one another other through TCP (Antonopoulos, 2014, p. 144). The Bitcoin protocol by itself is a communication protocol similar to TCP, and the overlay networks are built on top of Bitcoin similar how HTTP is built on top of TCP (Antonopoulos, 2014, p. 222). The block chain space has not agreed yet on a standard, so that means there is a variety of choice of protocols (Antonopoulos, 2014, p. 222).

The best example of a decentralized protocol is Bitcoin in its most popular implementation – Bitcoin Core (bitcoind). The protocol controls the validations and transactions, and it is not controlled by a third party. It makes use of the block chain as a source of data for past transactions.

It is also possible to develop other decentralized protocols on their block chains, as it is the case with the Ethereum protocol which claims to be able to execute Turing complete scripts (Wikipedia, 2017c), which help to write programs on the Ethereum's block chain that can solve problems by using sophisticated logic. Other good examples are Lazooz (http://lazooz.org/), a decentralized ride-sharing and OpenBazaar (https://openbazaar.org/), a decentralized marketplace. Also, there are other implementations of the Bitcoin protocol such as bcoin (http://bcoin.io/) and btcd (https://github.com/btcsuite/btcd).

2.2.3 Layer 2: Off-chain protocols

Some layer 2 technologies in block chain allow doing things off-chain in a decentralized manner allowing for more data to be executed than with doing things on-chain. Off-chain transactions are still anchored in the block chain. Layer 2 can be viewed as the application layer, "the HTTP" layer of block chains, which uses the chain for security (Stark, 2017). The application layer is a new layer in the model as the last step before the users and commercial businesses.

2.2.4 Layer 2: Overlay networks

Another layer 2 technologies are the overlay networks which work in parallel to the block chain. They perform tasks that the Bitcoin network cannot do (Monegro et al., 2014, "Overlay Networks"). They embed data into the block chain via transactions, which is later decoded using their network of nodes, aka embedded consensus. They are using the block chain to time-stamp or validate data. Examples of overlay networks are Counterparty (http://counterparty.io/), the OMNI layer (http://www.omnilayer.org) and side chains (https://blockstream.com/technology/). Those overlay networks benefit from the block chain because they can make use of the security that comes with the chain without needing to make a separate block chain. This layer can extend vanilla block chain to support other kinds of applications and eventually be capable of creating other currencies and side chains (vamsital, 2016, “Network Protocol Stack,” para. 2).

2.2.5 Layer 3: Users

In the future, there might be other technologies built on top of layer 2. It is still a work in progress. At the moment layer 3 is occupied by anyone interested to keep their wealth on the ledger and to transact with other peers without censorship or the need to know one another. Wallets, exchanges, payment processors also compose this layer. Independently of the type of wallet users have, they can talk (transact) to one another through the decentralized network, similar to sending an email from a different email provider.

2.2.6 Commercial APIs

To make it easier for businesses to take advantage of the protocol they would need Application Programming Interfaces (APIs). The average developer most likely cannot grasp the complexity of the protocol to build directly on top of it (Monegro et al., 2014, “Open Source and Commercial APIs”). Famous examples of APIs are Chain (https://chain.com/) for commercial uses, Blockchain.info and Coinpayments for payments

2.3 Public-key cryptography in block chain

Public-key cryptography exists since the 1970s, and it is a fundamental part of computer security ever since. Bitcoin uses ECC for deriving unique public keys from the private keys (Antonopoulos, 2014, p. 62). The calculation of a public key is irreversible and cannot be undone. The public key is used for receiving funds, and the private key for signing transactions to send those funds to another public key (Wilson, 2017a, p. 6). The relation between a private and public key allows for the creation of a digital signature that can be used to validate the public key allowing for outgoing transactions. The digital signature scheme is used to prove ownership of a public key without revealing the private key. When transacting, a user presents their public key and corresponding signature to the network; then the Bitcoin network can verify that the person owns the funds at the time of transfer (Antonopoulos, 2014, p. 62).

2.3.1 Private key

A private key gives rights for owning and controlling funds on the block chain. The private key is the password to the public key. The management of a private key is the most critical component in operating with a block chain. If a private key is lost, all funds controlled by that key are locked forever on the block chain. The private keys are used to create digital signatures that prove ownership and give access to transaction outputs. The transaction outputs contain the coins and scripts, and those outputs are stored in the block chain (Antonopoulos, 2014, p. 85). Furthermore, a private key should be backed up and kept in secret, because if a third party knows the private key, they have complete access to the funds (Antonopoulos, 2014, p. 63).

A private key is a 32 bytes (256-bit) random number, which can be represented in several ways, one of which is a 64 set of alphanumeric characters (Bitcoin Wiki, 2017e). The private key represents 256 numbers of 0's and 1's. A bit is a portmanteau of "**b**inary dig**it**" (Wikipedia, 2017a)**.** Therefore, the total amount of private key combinations is 2^{256}, which is a huge number, approximately 10^{77}. In comparison, "there are estimated between 10^{78} to 10^{82} atoms in the known, observable universe" (Villanueva, 2015), and around $7 * 10^{27}$ atoms in a 70 kg human body (Jefferson Lab, n.d.). More precisely, the total number of private keys can be any 256-bit "number between 1 and (n – 1), where n is a constant that determines the maximum value that can be turned into a private key ($n = 1.158 * 10^{77}$), defined as the order of the elliptic curve used in bitcoin" (Antonopoulos, 2014, p. 64). It is essential to use a good random number generator which uses methods in elliptic curve cryptography and which is a Cryptographically Secure Pseudo Random Number Generator (CSPRNG), so it does not have backdoors (Antonopoulos, 2014, p. 64). Humans cannot generate good random numbers (Figurska, Stańczyk, & Kulesza, 2008, p. 184). Anyone can create a Bitcoin private key, and that key will always be unique.

Everything digital is susceptible to hacking. A private key is secure from hacking because of big numbers. If people use strong random number generators, guessing the private key is virtually impossible. If no processing power is applied, the odds of guessing a private key are 2^{-256}. If computing power is used to list all private keys, and for each second a computer finds one trillion keys, then it will take $3.67 * 10^{57}$ years to list all possible keys (PSBlake, 2014). Moreover, to list all private keys, there will be a need for storage - 32 bytes per key, resulting in $2^{256} * 32$ bytes $= 3.70 * 10^{78}$ bytes of data. If the entire planet Earth is used as a hard drive to store all keys and the Sun as an energy source to power the drive, there will be a need for 3.70 * 10^{28} Earths and 2.37 * 10^{11} Suns (PSBlake, 2014).

Below it is shown an example of a private key (should not be used).

> *"Randomly generated private key.*
> *1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD"*
> *(Antonopoulos, 2014, p. 64)*

2.3.2 Wallets

Cryptocurrency wallets do not contain coins. Wallets are containers for private keys (Antonopoulos, 2014, p. 84). In the past wallets were creating a series of random keys and the user had to make frequent backups and copies of each key. Nowadays, there are new wallets which allow for the control of multiple private keys through Hierarchical Deterministic (HD) key creation. The HD wallets enable the creation of a chain of keys which are connected to one another. Each new private key connects to the previous one through a one-way hash function. To recreate the sequence of keys, a user only needs the first key (master key) (Antonopoulos, 2014, p. 84). Users can generate their master key from a seed, which is a one-way hash function of random numbers combined with some other data. The seed is sufficient to recover the full sequence of keys deriving from the master key. A single backup at the wallet creation is enough. The HD scheme allows for easier migration from one wallet software implementations to another because a user only needs the seed to recreate all keys (see **Figure 19)** (Antonopoulos, 2014, p. 86).

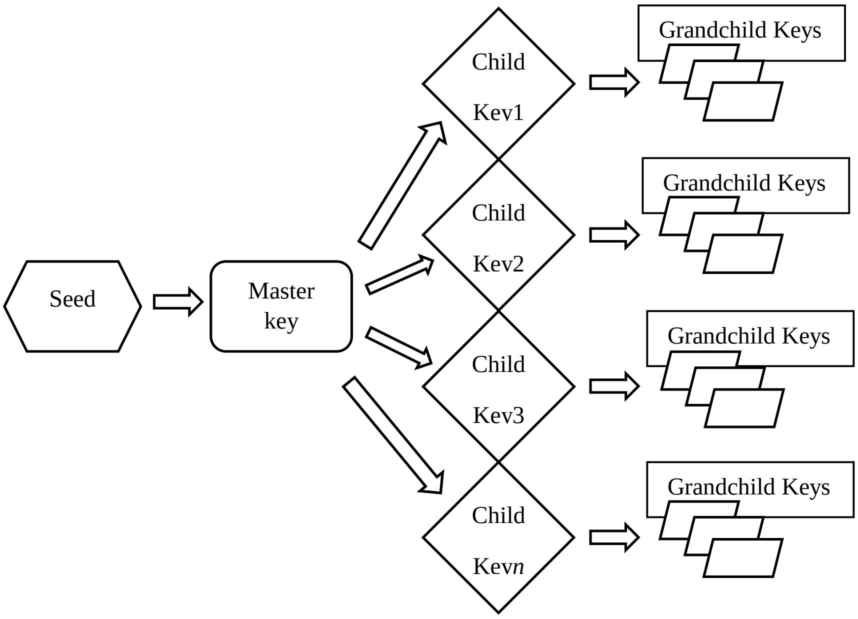


Figure 19: *Tree of generated private keys from a seed in HD Wallets (Antonopoulos, 2014, p. 88)*

HD wallets allow for the use of mnemonic codes (words in English) to recreate the seed. The words represent a random number. It is much easier to remember words than random numbers. The only backup a user must do is at the beginning to write down the mnemonic words. The words are the backup. He or she can then recreate the wallet and all associated private keys using those words using any HD wallet software.

Other types of wallets include paper wallets and multisignature wallets. Paper wallets are just private keys printed on paper. Usually, paper wallets are generated offline and printed from a printer that is not connected to the internet. It is an efficient way to store funds offline which is known as “cold storage” (Antonopoulos, 2014, p. 105). Multisignature wallets can generate multisignature public keys. It is a scheme where two or more private keys are required to spend the funds from a public key (Antonopoulos, 2014, p. 132). The multisignature scripting was created to allow escrow services where funds cannot be spent unless all parties agree (Bitcoin Wiki, 2017c). There is also the possibility for a multisignature paper wallet, which is a paper wallet that has two or more private keys printed.

Storing funds on the block chain is practically incorruptible, although to protect the funds one must safeguard his or her private keys. Securing the private keys in all block chain use cases is crucial. People do not own coins in the literal sense, and the wallets do not hold real balances (Wilson, 2016a, p. 5). They can only own the private keys which give them access to coin balances. A private key is similar to a certificate of ownership. Through the properties of the public-key cryptography, a coin only gives the ability to spend it irreversibly, or just to hold it. If numerous people know a specific private key, the person who is first to use that private key (exercise the spend ability) is entitled to the benefits of that spend according to the Prisoners’ Dilemma (Wikipedia, 2017f).

2.3.3 Elliptic curve cryptography

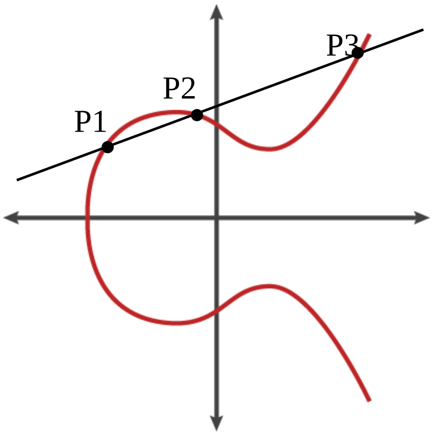


Figure 20: *Elliptic curve (Sullivan, 2013)*

Bitcoin uses ECC for digital signatures and for creating public-private key pairs. ECC is next generation public-key cryptography, invented by Neil Koblitz and Victor Miller in 1985 and "entered wide use in 2004 to 2005" (Wikipedia, 2017d, "History"). It comes after what is considered the first generation of cryptographic schemes, the Rivest-Shamir-Adleman (RSA) algorithm and Diffie–Hellman key exchange (D–H) (Sullivan, 2013, "The dawn of public key cryptography," para. 1). RSA was first described in 1977 (Wikipedia, 2017g) and D-H in 1976 (Wikipedia, 2017b). ECC provides a higher level of security while maintaining performance (Sullivan, 2013, para. 2).

Geometrically, if there are two points P1 and P2 on the elliptic curve (see **Figure 20**) and if a line is drawn between those two points, it will intersect the curve at a third point P3. A line between two points always intersects in one additional point on the elliptic curve (Antonopoulos, 2014, p. 68). If P1 and P2 are the same points, the line becomes tangent to the curve and still interests at a third point. There is also the case when the line is vertical (P1 and P2 have the same x-value but different y-values) then the intersect will be at infinity (Antonopoulos, 2014, p. 68).

The equation defining elliptic curves is $y^2 = x^3 + ax + b$, where a and b are elements of the field K. Some examples of K are the real numbers, rational numbers, complex numbers and the integers modulo p. The characteristics of the cryptosystem define a and b. Bitcoin uses the "secp256k1" standard for its elliptic curve where $a = 0$ and $b = 7$, therefore the equation becomes: $y^2 = x^3 + 7$, or more precisely: $y^2 \bmod p = (x^3 + 7) \bmod p$ (Antonopoulos, 2014, p. 66).

“Secp256k1” is a published standard but it is rarely used outside of Bitcoin (Narayanan et al., 2016, p. 40). For example, in Transport Layer Security (TLS) for secure web browsing, it is used the more common “secp256r1” curve (Narayanan et al., 2016, p. 40). The decision to use “secp256k1” was made in the early days of Bitcoin, and it is hard to change now. There is no fundamental reason behind that choice (Narayanan et al., 2016, p. 40). Some fear that with time the algorithm might be broken by an unexpected attack. The fear is based on the assumption that it might be difficult to change to support new cryptographic algorithms at a later stage. It would require extending the Bitcoin scripting language (Narayanan et al., 2016, p. 96).

The math behind ECC is complicated and beyond the scope of this research. Other variables also need to be included in the model. The research does not focus on the math. The power of ECC lies in the fact that it is easy to calculate the third point on the curve. However, if someone knows the third point, it is close to impossible to find where the other two points are. By knowing only the third point, there is a tremendous number of possibilities for where the intersect of the two points is on the curve.

2.3.4 Public key

Users calculate public keys through the wallet software or other means. The public keys ape deriveд from the private keys through elliptic curve multiplication. The generation of a public key is an irreversible process. If someone tries to reverse it by a brute-force, to obtain the private key, the operation would be as tricky as trying all possible private keys (Antonopoulos, 2014, p. 65).

The formula is: public key = private key * generator point. Generator point is part of the secp256k1 standard, and it is always the same for all keys in Bitcoin (Antonopoulos, 2014, p. 68). The math behind the generation of a public key is unnecessary for this research. All bitcoins in circulation belong to an individual public key. However, the public key is not the same as a bitcoin address.

2.3.5 Bitcoin address

A Bitcoin address looks like this: 18vunmbzXuZj5iMwK8Nt1V5b8JNmWhamSQ

All bitcoin addresses are generated from the public keys through a one-way hash function (Antonopoulos, 2014, p. 71). Addresses are 26-35 alphanumeric characters which are shorter than public keys which can have 51 characters. Also, addresses are standardized; some addresses start with “1” or with “3,” each standard comes with different script conditions for unlocking the coins (Bitcoin Wiki, 2017e).

Private key → Public key → Bitcoin address

2.4 Transactions

Bitcoin transactions contain inputs (source of funds) and outputs (destination of funds). Transactions are hashed using SHA-256, and this creates a unique transaction ID (Bonneau et al., 2015, p. 106). Each output contains a numeric value which is the number of coins (Bonneau et al., 2015, p. 106). Coins can be fragmented into small bits up to 100th million of a bitcoin (10^{-8}), and the smallest unit is called a “satoshi.” Bitcoin is typically denoted as BTC or XBT (Bonneau et al., 2015, p. 106). Each output also contains scripts written in a special scripting language which is called “scriptPubKey” (Bonneau et al., 2015, p. 106). The scripting allows for building conditions for transactions to be unlocked and spend. The output is included as input in the following transaction (Bonneau et al., 2015, p. 106). The output scripting allows for many other use cases to develop that would require more complex logic such as distributed contracts (Bitcoin Wiki, 2017b).

The fee that is paid to the miners which include the transaction in the block on the ledger is equal to the difference between the inputs and outputs (Robla, 2015, p. 5). In Bitcoin, inputs can only be spent in full. Therefore, users send change outputs back to themselves when they send different amount than the input. For example, if someone wants to send 2.4 BTC from two addresses containing a total of 3 BTC, he or she has to send 2.4 BTC to the payee, 0.599 BTC to self and 0.001 BTC to the miner (see **Figure 21**).

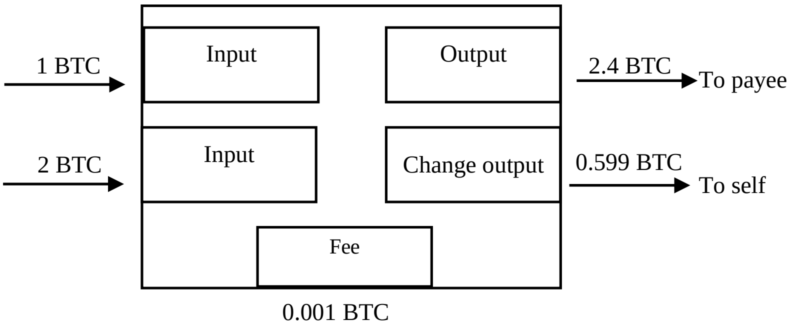


Figure 21: *Structure of a transaction (own model)*

2.4.1 Anatomy of a block chain transaction

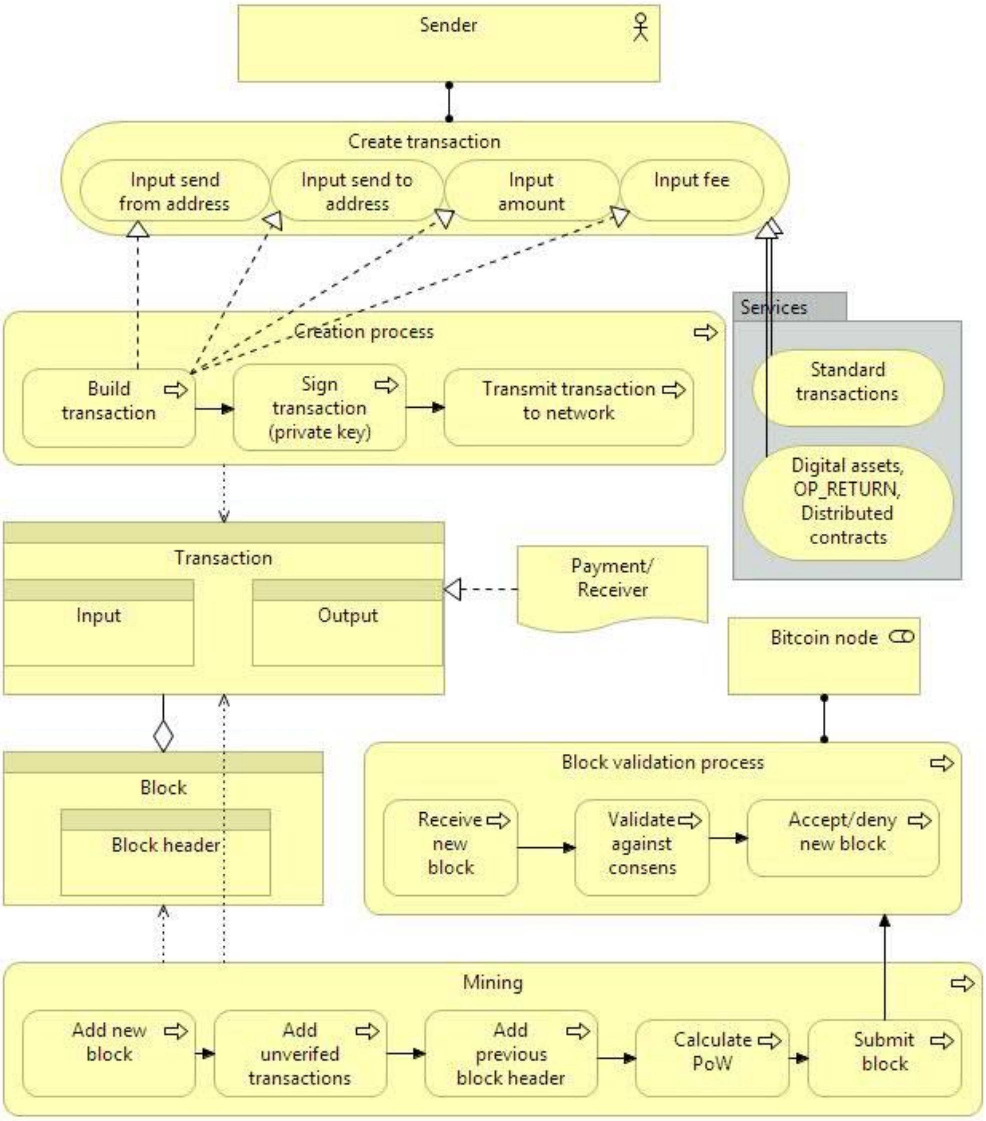


Figure 22: *Transaction creation and confirmation (own model)*

Users can create transactions which they also sign and broadcast to the network. **Figure 22** presents some of the primary services for transactions – standard transaction and transactions with special conditions (e.g., digital assets, contracts, OP_RETURN transactions). The three processes in this example are creation process, block validation process, and mining. The creation process includes the building of a transaction and transmitting it to the network. First, the sender puts the amount, the receiver's address (this address determines the conditions of the transaction), the address from where to send and the miner's fee. Second, the software constructs the transaction, and the user signs the transaction with his or her private key. The signed transaction is transmitted to the neighboring nodes for validation (Antonopoulos, 2014, p. 182).

The validation processes of a transaction are repeated until it reaches (almost) every node in the network. Nodes keep the unverified transactions in a memory pool (mempool) (Antonopoulos, 2014, p. 28). If a transaction is invalid, the propagation process will stop.

After a transaction is validated, miners add it to a block. Then, they calculate the PoW and submit the new block to the network. Each node will validate whether the newly mined block respected the consensus rules. Newly validated blocks are then stored locally on the nodes until they assemble a chain connected to the existing block chain. “The independent validation of each new block by every node on the network ensures that the miners can’t cheat” (Antonopoulos, 2014, p. 202).

Once recorded on the block chain the transaction is a permanent part of the ledger and is accepted as valid by all participants. The funds can then be spent in a new transaction (Antonopoulos, 2014).

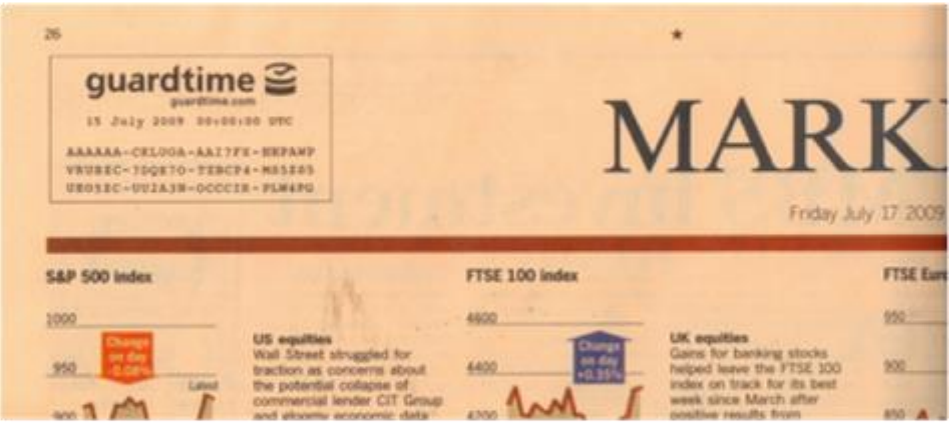
2.4.2 Trusted time-stamping on a block chain

Time-stamping creates an order when documents were created. Interestingly, Haber and Stornetta’s data structure for linked time-stamping is borrowed in Bitcoin with the difference that in Bitcoin time-stamping is secured by the PoW (Narayanan & Clark, 2017, p. 5). The proposed scheme by Haber and Stornetta is linking hashes of documents together into a chain with pointers backward in time anchored to a Time-Stamping Service (TSS) (Haber & Stornetta, 1990, p. 110). The authors aimed at building eventually a “digital notary” which could be used for patents, business contracts, and any other use cases that require proof that a document was created at a particular point in time. (Narayanan & Clark, 2017, p. 5). They even mention that the same idea could apply to subsequent financial transactions (stock trades, currency exchanges) (Haber & Stornetta, 1990, p. 107).

Digital documents are easy to tamper with, and the modification can leave no trail or sign on the physical medium (Haber & Stornetta, 1990, p. 100). The purpose of TSS is to be an arbitrator when the integrity of a document is challenged. When a user wants to time-stamp a document he or she uploads the document to a TSS. The service records the date and time the document was received and retains a copy of the document for safe-keeping (Haber & Stornetta, 1990, p. 101). The uploaded document can later be compared with the original to detect any tampering (Haber & Stornetta, 1990, p. 101). This is an explanation of the most fundamental mechanism of time-stamping in which Haber & Stornetta (1990) identify five possible problems: bandwidth, storage, privacy, incompetence and trust (p. 101). To solve these problems, the authors propose two improvements – hash functions and digital signatures.

Instead of transmitting the entire document to a TSS, the user can send a hash of the document. Consequently, to validate the authenticity of the document, it will require to produce the hash form the original and verify if it satisfies the hash on the TSS. The procedure of validating hashes solves the problems with bandwidth, storage, and privacy (Haber & Stornetta, 1990, p. 102). The second improvement is digital signatures because they allow for unique identification of messages sent by a signer. When the TSS receives a hash, it adds the date and time and then signs the data and gives it back to the user in the form of a "certificate." Then, the user can check the signature of the certificate to be assured that the TSS was the one who completed the request, and that "the hash was correctly received, and that the correct time is included" (Haber & Stornetta, 1990, p. 102). Digital signatures take care of the problem with incompetence and trust.

One of the first implementation of the Haber & Stornetta (1990) time-stamping scheme, was by a company called Guardtime, started in 2007. Instead of hashes, Guardtime was publishing the Merkle roots as ads in a newspaper (see **Figure 23**). The values can be published in any "hard-to-modify and widely witnessed media" (Buldas, Kroonmaa, & Laanoja, 2013, p. 4)



26

guardtime
guardtime.com
15 July 2009 00:00:00 UTC

AAAAAA-CRLUOA-AAI7FX-HHPAMP
VRUBEC-3DQE7O-TEBCP4-MS5E65
UE03EC-UU2A3N-OCCCIR-PLM4PG

MARK

Friday July 17 2009

S&P 500 index

US equities
Wall Street struggled for traction as concerns about the potential collapse of commercial lender CIT Group and gloomy economic data

FTSE 100 index

UK equities
Gains for banking stocks helped leave the FTSE 100 index on track for its best week since March after positive results from

FTSE Eur

Figure 23: *Guardtime Merkle root in a newspaper (Narayanan & Clark, 2017, p. 8)*

Instead of block chain, Guardtime was using newspaper. Moreover, the Merkle trees are used to capture many different pieces of hashes or data into a single hash – the Merkle root. The Merkle trees allow for proving that any of those pieces are included in the root. Nowadays, Guardtime is working on the Keyless Signature Infrastructure (KSI) ledger for enterprises and is considered one of the world's largest block chain companies by revenue.

Time-stamping on a block chain instead of a newspaper requires to send money to the hash of the data instead of the public key which results in burning the coins; it makes them unspendable. Those transactions are stuck on the block chain because no one knows the private key corresponding to that address. Therefore, only small amounts are transacted to keep the costs low (Narayanan et al., 2016, p. 240). The cost for committing hash data into a transaction can be reduced by using a single commitment for multiple values. Almost all block chain time-stamping services collect the commitments for a given day from all users to combine them into a large Merkle tree and publish the Merkle root in one unspendable output (Narayanan et al., 2016, p. 241).

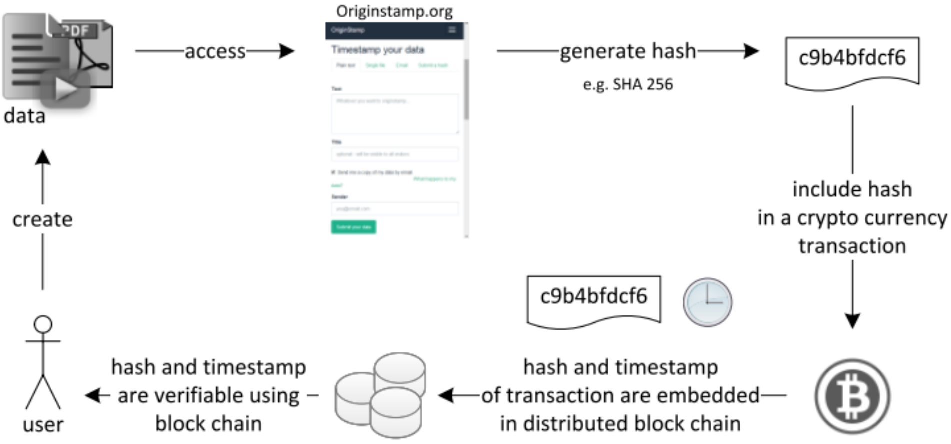


Figure 24: *Trusted time-stamping using cryptocurrencies (Gipp, Meuschke, & Gernandt, 2015, p. 3)*

Figure 24 illustrates an example of a block chain time-stamping service which allows users to submit digital content through the web. When submitting a file, a script creates a hash of the data. The hash is then converted into a Bitcoin address where the user can send coins to anchor the output in the block chain (Gipp et al., 2015, p. 3). The hash function ensures that if one single value of the file is changed, it will generate a different hash. To verify the data, the process of creating the time-stamp has to be replicated, and the result has to be compared with the block chain hash (Gipp et al., 2015, p. 3).

2.4.3 Non-monetary transactions

Block chains are not suited for storing vast amounts of data. In Bitcoin transactions are limited in size (up to 4MB) for the purpose that people do not start congesting the block chain with data. The block chain incentive model requires paying enormous fees for storing big data and therefore can be somewhat inefficient. Some experimental platforms deal with decentralized data storage such as Filecoin (IPFS) and SiaCoin.

Non-monetary transactions are transactions that contain additional data to the value data and do not always result in the transfer of funds between peers. Usually, those transactions are burned (spent to address without a private key). Bitcoin uses Operation Codes (Op-code) from its script language to create transaction outputs with conditions. Some of those scripts can push data or perform functions within a public key script or signature script (Bitcoin Wiki, 2017d). Bitcoin uses the OP_RETURN scripting for storing data allowing for embedding metadata into transactions (Rauchs & Hileman, 2017, p. 27). Such transactions then become carriers of information that have a meaning outside of the network, which in a sense can serve the purpose of a decentralized time-stamping tool for keeping records (Rauchs & Hileman, 2017, p. 107). There are cryptocurrency systems that only exists for specific non-monetary use cases (decentralized domain name registry or a decentralized computing platform). The native currency in such systems is only used to incentivize the miners to keep the system secure (Rauchs & Hileman, 2017, p. 105).

Since the introduction of the OP_RETURN feature in Bitcoin embedding metadata in transactions has increased (see **Figure 25**) (OP_RETURN Stats, n.d.). This is a new standard output type. An OP_RETURN adds up to 40 bytes of user-defined data to any transaction. The non-monetary use of Bitcoin has increased which encourages vendors to create more tools and applications around this use case. The OP_RETURN scripting purposely returns an error when executing so that it can never run successfully so that data included in the output is ignored. This allows for putting any data in the transaction output (Narayanan et al., 2016, p. 241). Some consider that the OP_RETURN is “polluting” the block chain with transactions that are outside its original intent which is to provide a record of financial transactions and not record for arbitrary data (Narayanan et al., 2016, p. 298).

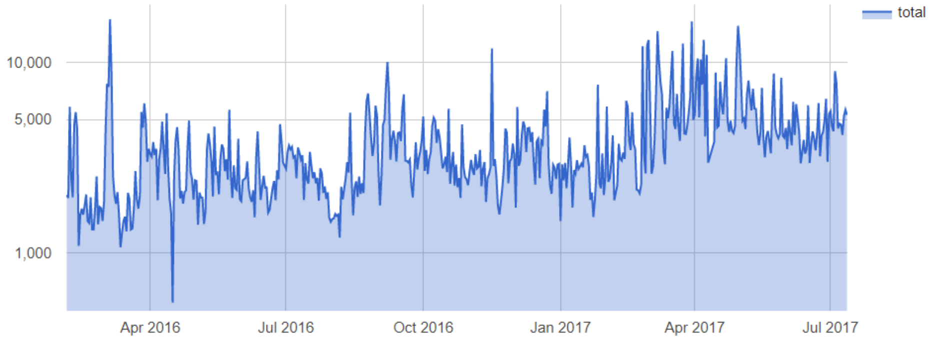


Figure 25: *Usage of OP_RETURN in Bitcoin transactions (OP_RETURN Stats, n.d.)*

2.4.4 Off-chain and on-chain transactions

Off-chain transactions do not modify the block chain because they do not happen on the block chain. Value is moved outside the block chain. On-chain transactions directly alter the block chain and are usually referred to as just transactions, and they depend on the block chain to define their validity (Bitcoin Wiki, 2016c, para. 1). Off-chain transactions rely on other methods of defining their validity and recording them. On-chain transactions are accepted by trusting that the majority is "honest" and will not attempt to reverse the transaction (Bitcoin Wiki, 2016c, para. 2).

An off-chain transaction is not public. Systems for managing off-chain transactions can record them instantly as they happen. Example of an off-chain transition is when two parties agree to transact offline by exchanging private keys. Another example is by using multisignature techniques (Bitcoin Wiki, 2016c, “Methods”).There is also the possibilities of using payment channels among peers for instant transactions. Payment channels are an upcoming new use case for Bitcoin.

3 Use cases

This chapter focuses mainly on potential uses cases beyond payments in block chain. There is also a section for the prevalent use case of value transfer. The last two use cases are dedicated to legal record keeping and health care which are also discussed in detail in chapter 4.

Giaglis & Kypriotaki (2014) call for an agenda to research future use cases of digital currencies because they believe the "future uses of the block chain concept will be flourishing in a highly increasing rate" (p. 9). They envision their agenda for the discipline of Information Systems research on digital currencies and Bitcoin "to assist the transition from the first era of applications" (cryptocurrency) to more disruptive uses of block chain applications (smart contracts) (Giaglis & Kypriotaki, 2014, p. 3).

3.1 Smart contracts

Smart contracts were introduced by Nick Szabo in 1996. Szabo proposed that digital bearer instruments can help create a digital equivalent of legal contracts, which could also be automated (Szabo, 1996, "Problems with Certification," para. 3, "Conclusion"). With the current success of the block chain, smart contracts are close to becoming a reality. Technically, a Bitcoin transaction could be considered a smart contract, because each output comes with conditions, which if satisfied can allow the user to redeem the funds. Bitcoin's programming language is restricted, and users can only choose pre-defined script templates. Ethereum allows for any level of programming to be incorporated in a transaction output. It offers the freedom to determine any condition. Smart contracts can be seen as an evolution of digital bearer protocols (Narayanan & Clark, 2017, p. 21).

One of the most fundamental smart contracts is nLockTime which is a transaction with a redemption date. Multisig is a smart contract where multiple parties agree on transferring funds, which allows for payment channels, betting, and many other use cases. Lastly, Atomic Swaps provides a riskless exchange of one digital asset for another, also called cross-chain swap. Smart contracts are business logic expressed in code. They guarantee the transfer of funds, if all conditions are met and if an asset is presented on the block chain (Narayanan & Clark, 2017, p. 21).

3.1.1 Contractual agreements

Investing in shares requires both counterparties to hold a bank account. Shares on a distributed ledger can be instantly settled which makes it easier to receive dividends and vote for proposals. Shares can be substituted on the ledger with meta-tokens, similar to a digital share certificate instead of a paper certificate. Distributed smart contracts make it possible for special conditions and classes of shares for these tokens. In derivatives, it can be even possible to program the execution of settlements following external events. Every contract can be coded in a token (ENISA, 2016, p. 25).

3.1.2 Automated companies and investment vehicles

Smart contracts on a distributed ledger can automate corporate activity, including governance, shareholder listing, recording board decisions and allocating assets. Smart contracts can also subject automated investment vehicles to regulatory requirements automatically and manage the holdings of the business with full transparency (ENISA, 2016, p. 27).

3.1.3 Smart properties

Smart properties would use the block chain as an inventory tracking and exchange mechanism for hard assets, real-world assets such as diamonds, cars, or it can be used for verifying the authenticity of goods (Lindman, Rossi, & Tuunainen, 2017, p. 1535; BitFury Group, 2016, p. 13). A smart property represents ownership over the hard asset. For example, a car would only operate if the driver holds the block chain token. Such technology is far from ready, it would be very slow with today’s block chains and poses many security risks. It requires implementation of dedicated ownership protocols on top of Bitcoin or another block chain, which are not yet developed (BitFury Group, 2016, p. 13).

3.1.4 IoT enabled devices

Block chain would be able to facilitate connected devices. Financial institutions can obtain real-time data from a range of matters such as adverse weather (for insurers), client location (fraud prevention), production facility status (valuation of business) (ENISA, 2016, p. 25).

3.1.5 Regulatory compliance

It is easy to calculate in near real-time the financial position of an institution on the block chain and predict future outcomes of accepting additional transactions regarding the risk management and capital requirements of a company. If permissioned block chains are to be used regulators would be able to enforce sanctions and closing the access to specific markets (ENISA, 2016, p. 27).

3.1.6 Auditing information

Tax audits and company accounting audits can be reported to regulators in real time instead of cyclical periods (ENISA, 2016, p. 25).

3.2 Value transfer

The principal use case of a block chain, for now, is the censorship-resistant value transfer. There is no single financial institution tracking the ownership of funds. The block chain maintains all records at all time of users' holdings.

The European Union Agency for Network and Information Security (ENISA) (2016) views block chain as a reformer of financial institutions. It is a distributed ledger technology which can improve the speed and cost of doing business "by simplifying back-office operations and lowering the need for human intervention" (ENISA, 2016, p.5).

3.2.1 Instant transactions

Transactions in Bitcoin usually take 1 hour to verify and confirm to avoid any double spend attacks, and credit cards take two to three days to confirm a transaction. Bitcoin is much better regarding the speed of confirmation, but it can be made even better with the "Lightning Network" (Lin & Liao, 2017, p. 657). Lightning creates a network of micropayment channels which allows for a low fee, near-instant secure transactions. These channels operate on Bitcoin by using op-codes to enable the riskless transfers. (Poon & Dryja, 2016, p. 55).

3.2.2 Proof of funds

A user can sign a message with the private key on the block chain proving they are the owner of funds (proof of funds). The user needs to show the address where the funds are stored and then sign a message with the private key. The other parties will be able to verify whether the signature corresponds to the address (ENISA, 2016, p. 25).

3.3 Legal record keeping

In its broad sense, a public notary is an authority that guarantees and certifies documents or identities. Thus far, identity on a block chain is still a problem, so the scope of a block chain notary is limited to only certifying and verifying of documents for proof of ownership and proof of existence. Proof of identity is a hard to solve problem because a private key does not grantee the identity of a person. Therefore, an actual notary on a block chain is still far from being a reality. This research discusses the block chain use in time-stamping and verifying of legal records.

Some of the legal records that could be on a block chain include titles, birth certificates, voting or court records (Lindman et al., 2017, p. 1535). A legal record can be any document that is public or private and relates to the conduct of the government (e.g., permits). Other government-licensed assets that could be digitalized on a block chain are houses, vehicles, and patents (Shelkovnikov, 2016, p. 1).

According to the American Land Title Association, there are around 30% mistaken land titles in property transactions (Schneider et al., 2016, p. 34). A presumption exists that this error is partly due to the paper-based nature of registration, recording, and administration of land titles. Moreover, any real estate related data like mortgages, leases or court orders, are recorded in a "chain of title," which exposes the integrity of information to human error and breaches the privacy of individuals (Schneider et al., 2016, p. 34).

In other areas of the world, property transfer fees are very high. In countries like Brazil, owners are paying up to 4% of the property value in transfer fees (notary-1.25%, registration-0.75%, legal fees-2.00%). Real estate broker fees are from 3% to 6% and transfer taxes from 2% to 4%. The total of transaction costs is up to 9%-14% in that country (Schneider et al., 2016, p. 34).

Some believe that registering property titles on the block chain could increase efficiency and prevent fraud (forged document transfers of property to false owners) and mistakes. It will save fees and improve data integrity and privacy. Property transactions on Bitcoin would require "colored coins," which operate on the overlay network (layer 2) on top of the protocol through the OP_RETURN scripting. The coins are colored because they represent a specific real-world asset in a digital format, they are programmed with unique functions different than the standard coins. The exchange of the colored coins is similar to standard coins. The private keys serve as cryptographic identities for moving the digital assets, and the title and identity documents proving ownership are hashed in a colored coin transaction (Shelkovnikov, 2016, p. 2). However, a loss of private keys would lead to loss of identity and therefore loss of ownership (Barbieri & Gassen, 2017, p. 8).

All property information is assigned to a transaction output. Before putting the information on the block chain, there must be a consensus over the legal owner, plot size and boundaries of the land (Barbieri & Gassen, 2017, p. 10). Further, there is also the possibility of a block chain ban by a state, and so the owners would lose their property rights (Barbieri & Gassen, 2017, p. 12). There is a good reason why third parties control the registries of land and the tracking of ownership exchange and why such systems are kept and supervised by the government. Such agencies and notaries are there to make sure that the information being entered in the registries is accurate and complete. Those third parties are also responsible for the verification of the authenticity of the documents which is there to prevent fraud. The liability of who controls the input into the block chain and the supervision of these controllers is still unclear (Barbieri & Gassen, 2017, p. 12).

Table 2: *Block chain time-stamping services*

Concept/Company	**Host**	**Link**
ChainPoint/Tierion	Cryptosystem	https://tierion.com/chainpoint
OpenTimestamps	Web/Self	https://opentimestamps.org/
Proof of Existence	Web	https://poex.io/
CryptoGraffitiy	Web	http://www.cryptograffiti.info/
Originstamp	Web	originstamp.org
BTProof	Web	http://www.btproof.site/
Tangible	Web	http://tangible.io/en/index.html
BitcoinTimestamp	Self	https://github.com/fireduck64/BitcoinTimestamp
ChronoBit	Self	https://github.com/goblin/chronobit
Stone	Self	https://github.com/dasmithii/stone
Stampery	Web	stampery.co
Blockchain Identity	Self	http://jrruethe.github.io/blog/2015/02/28/blockchain-identity/
Factom	Cryptosystem	http://factom.org/
Btc-PGP	Web	http://royalforkblog.github.io
Stampd	Web	http://stampd.io

Table 2 shows some of the services for data proofs and time-stamping on a block chain. One of the researched companies was Tierion. Tierion's API can work on multiple chains by making a proof that can be used to verify the integrity and time-stamp of any data, file, or business process. After anchoring the data on a block chain, anyone can verify it by using open source tools (Tierion, 2016, p. 4). More information about Tierion can be found in section 4.2 and **Appendix C**.

Solely relying on hashes for proofs is not enough. In January 2017, Julian Assange wanted to prove he was alive and disprove the rumors that he was dead. He used Bitcoin's block chain for that purpose (Hertig, 2017). He recorded a video of himself where he was reading out the latest block height (block hash) at that time. This action is similar to making a video and showing the latest newspaper (Wilson, 2017b). His action shows that he needed an additional security process to prove his existence (the video) and could not do it only with the block chain (Wilson, 2017b). Furthermore, there are other equally persuasive and better ways to do that (video and newspaper, video and the current price of a stock) (Wilson, 2017b).

On the block chain, proof of existence is the creation of a digital signature by the owner of a private key. A signature proves that a specific private key existed at a specific time. However, a block chain cannot prove who controls that key. The original purpose of the block chain was “to remove any central oversight of keys and account holders” (Wilson, 2017b).

To embrace non-currency use cases, the block chain alone cannot do that; it needs outside processes. Adding other security processes to the already complex, redundant and inefficient way it works, would only make things even more convoluted. There could be other means to accomplish similar outcomes in a simpler way (Wilson, 2017b).

Before using a block chain in record keeping, advocates of the technology have to address some serious issues with the authentication and identification of users and also how to protect against loss of private keys (Barbieri & Gassen, 2017, p. 13). Block chain advocates need to understand the importance of the relation among the roles of the cadaster, the land register and the notary in the preventive administration of justice (Barbieri & Gassen, 2017, p. 13).

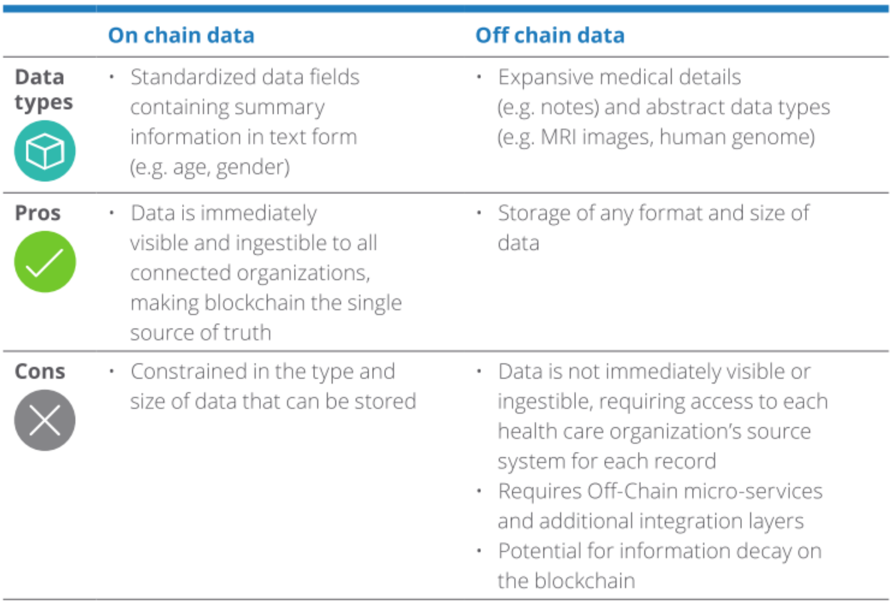
3.4 Health care

One of the renowned reasons to use a block chain in health care is the presumption that it will strengthen data integrity and preserve patients’ digital identities better than standard systems, because of public-key cryptography, proof of work, and distributed data, which are inherent properties of block chains (Krawiec et al., 2016, p. 6). People also proclaim that it could potentially improve data interoperability (Krawiec et al., 2016, p. 3).

In the USA in 2015 and 2016, there were 113 million and 3.9 million individuals respectively (U.S. Department of Health & Human Services, 2017), affected by data breaches in health care. Breaches of private information in health care remain at high levels (Beltran-Aroca et al., 2016, p. 2). There is a threat to the confidentiality of patients. It is considered a problem that clinical professionals encounter regularly. Beltran-Aroca et al. (2016) argue that there is one breach per 62.5 hours in Spain (p. 11). The loss of confidential data due to lack of security or hacking has negative implications for the doctor-patient relationship (Beltran-Aroca et al., 2016, p. 11).

The idea of using block chain in health care revolves around utilizing the public and private key pairs as identifiers for unlocking patients’ private data. The private key is the secret to the openly visible public key. Patients prove their identity (public key) through the private key (Krawiec et al., 2016, p. 6). The block chain would serve as a permission layer for unlocking and sharing “identity attributes with specific health care organizations” (Krawiec et al., 2016,

p. 7). The information will be shared within the health care system “on as-needed-basis” to reduce vulnerabilities from storing Personally Identifiable Information (PII) on multiple locations. (Krawiec et al., 2016, p. 7).



	On chain data	Off chain data
Data types	• Standardized data fields containing summary information in text form (e.g. age, gender)	• Expansive medical details (e.g. notes) and abstract data types (e.g. MRI images, human genome)
Pros ✓	• Data is immediately visible and ingestible to all connected organizations, making blockchain the single source of truth	• Storage of any format and size of data
Cons ✗	• Constrained in the type and size of data that can be stored	• Data is not immediately visible or ingestible, requiring access to each health care organization’s source system for each record • Requires Off-Chain micro-services and additional integration layers • Potential for information decay on the blockchain

Figure 26: *Information storing on a block chain in health care (Krawiec et al., 2016, p. 6)*

Figure 26 is taken from Deloitte’s report “Blockchain: Opportunities for Health Care” (2016) and shows the way data is expected to be handled in a health care block chain. The size of the information is of concern. Naturally, doctor notes and other free submission materials could create large transaction sizes which will harm the performance of the chain. To operate normally and manage the performance of the block chain there needs to be a limited and standardized set of data (Krawiec et al., 2016, p. 8). Small data such as personal information about a patient will be stored directly in the block chain (on-chain), and comprehensive medical details will be kept in separate, traditional databases (off-chain) and only links to that data will be retained on block chain to act as pointers. Storing large files on the chain slows down processing speeds and will worsen the scaling of the system. Medical information on the block chain is believed to be secure, and the peers who are permissioned to access the chain will be able to view that information (Krawiec et al., 2016, p. 6). In the USA, identity, PII and Protected Health Information (PHI) on a block chain should be separated and encrypted into segregated entities, so that it satisfies the HIPAA Privacy Rule[9] (Krawiec et

[9] “The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically” (U.S. Department of Health & Human Services, 2015).

al., 2016, p. 9). However, some are certain that personal information and PHI do not belong in a block chain because of the transparency of public block chains (Wilson & Chou, 2017, p. 6).

To understand the costs of a fully scalable block chain customized for Health and Human Services (HHS), there need to be more targeted experiments, tests and block chain guidelines (Krawiec et al., 2016, p. 9). In health care, computing power for processing all transactions, logically, should be outsourced to the government (e.g., the HHS in the USA). The HHS should be paying the costs of the block chain. However, the HHS then becomes the owner of the block chain, and thus the value of decentralization disappears (Krawiec et al., 2016, p. 8).

Significant pitfalls of using block chains in health care are the vendor lock-in (it becomes costly to move to another system, vendors control customer data and can raise prices), the tokenization of projects and the block chain hype. There is a certain degree of immaturity in the technology, and associated risks with patients not being able to provide their health records if their keys are lost. Patient information security, privacy, and ownership of their records are good things. However, there are risks when a patient is incapacitated, or their private keys get stolen or lost, and permission is required to access their health records (Tierion, 2016, p. 7).

An ideal scenario would be not to build a proprietary solution from scratch and instead wait for established software vendors to integrate new technologies (Tierion, 2016, p. 5). In health care, the life of patients depends on what technology professionals choose. Block chains are not immune from security risks and are also attacked just like other technologies. For example, in Ethereum an attacker was able to exploit a smart contract and extract $60 million (Tierion, 2016, p. 6). The increased interest in this technology can bring opportunities to create new standards for managing health care records and patient data and optimize interactions between health care and insurance companies. Consortiums are possible to form in such case to create standards (Tierion, 2016, p. 4). Even if no block chain solution gets adopted, the interest itself in the technology could inspire other possible alternatives to become a reality. Such new networks are not required to use block chain technology (Tierion, 2016, p. 4).

Contrary to Deloitte’s believe, some think that block chains will not solve electronic health care problems and will not improve data interoperability. Originally, block chains were not designed to solve such problems (Wilson & Chou, 2017, p. 8). Public-key cryptography can be accomplished without a block chain. Public-key cryptography can produce the same result of knowing who is who without miners and nodes. Furthermore, a private key does not guarantee that the person holding it is the “real” person (Wilson & Chou, 2017, p. 7). The purpose of Bitcoin’s block chain is to be trustless, meaning that it is unimportant who holds the key, whereas in health care it is essential. Carers, researchers, insurers, and patients need to be adequately authorized (Wilson & Chou, 2017, p. 7).

3.4.1 Portable identity

Cryptography in distributed ledgers allows participants to produce their own identity by generating a private key. Their private key is their identity on the block chain. As long as they do not generate more private keys their identity stays the same. This process allows them to port their identity to different services that use block chain (ENISA, 2016, p. 27). However, the private key can also be used by a different person.

An exciting project for identity on the block chain is Ping Identity which has invested in a company called Swirlds. Swirlds uses new block chain inspired technology called “hash graph,” which presents a more efficient system than a block chain. Ping will be working with Swirlds to solve problems in identity management. As a first step, they will focus on Distributed Session Management (DSM), which is a system for globally signing off from multiple sessions on the web. This would be useful for hacked users who lost their passwords to shut down their accounts (Wilson, 2016b).

4 Expert interviews

In this chapter, the results of the interviews are presented, and in section 4.11 there is an analysis of the findings. A panel of interviewed experts is revealed in **Table 3**.

The main interview questions follow a pattern which is in line with the main research question. The main interview questions are an archetype of the detailed questions found in **Appendix K**.

Main interview questions:

1. What factors drive organizations believe they need block chain?

2. What are the current technological impediments blocking block chain implementation?

3. What is the current progress on block chain implementation?

4. What are the overall costs for a block chain implementation?

5. What are possible developments after implementation?

6. How would organizations measure progress and efficiency of a block chain?

Two of the interviewed experts work for clinics and research facilities, and another expert works for a notary organization. Critics and software developers were also interviewed. It is almost impossible to obtain the contact information of people working with block chain. Wayne Vaughan, CEO of Tierion, stated that most of the block chain projects are not public. Publically available data is only the “tip of the iceberg.” He mentioned that usually, Tierion’s clients ask to sign NDAs and do not like talking in the open about the work they do, or how they use the technology.

Table 3: *Experts panel*

Name	Institution	Position	Field of expertise
Jelle ten Hoeve	Netherlands Cancer Institute (NKI)	Head of Research IT	Genomics
Wayne Vaughan	Tierion / Chainpoint	CEO, Founder	Data proofs, verifications, time-stamps
Robert Currie	Genomics Institute (UCSC)	CTO	Genomics, block chain, and cryptosystems
Jasper Roes	Het Kadaster	Senior Advisor	Products and processes, open data, permits, block chain
Maarten Everts	University of Twente	Research Scientist at TNO	Information security, applied cryptography
Stephen Wilson	Constellation Research	VP and Principal Analyst	Digital identity and privacy
Christopher DeRose	DeRose Technologies, Bitcoin Uncensored (YouTube)	Owner & Software Developer	Software and block chain journalism
Erich Erstu	Cryptograffiti.info	Owner and Developer	Proof of existence, record-keeping (encode hidden messages, uploads)
Jaco van de Pol	EEMCS (University of Twente)	Head of Department Computer Science	Computer science
Maqsood Ahmed	PACCAR (truck manufacturing company)	Technical Fellow	Technical support and administration

4.1 Interview with Jelle ten Hoeve (Preliminary research)

An interview with Jelle ten Hoeve, Head of Research IT from the Netherlands Cancer Institute (NKI) was conducted to gain a better understanding in life-science data exchange and Health Information Exchange (HIE).

Over the past decades, comprehensive cancer centers have provided research information to health care professionals and the public mostly independently or in small collaborations. However, recently, under the directive of Joe Biden, several initiatives for (global) genome health care data sharing were brought together. Examples, in which the NKI takes part, are the American Association for Cancer Research - GENIE project and the Cancer Gene Trust (CGT) of the Global Alliance for Genomics and Health. The purpose is to share variables between parties and the public because large datasets are needed to provide professionals the data required to develop precision/personalized treatments. The CGT project is hosted in a distributed way using the IPFS protocol, and parties can access the data. The distribution of patients data will eventually allow cancer patients to be the owners of their records and choose whether to contribute to cancer research with their information. They can be supplied with a private key to where their data is stored in a transaction in the block chain. Then, if they want, they can send the data to the clinic for research. Please refer to **Appendix B** for more details of the interview.

4.2 Interview with Wayne Vaughan (Preliminary research)

Wayne Vaughan, the CEO of Tierion and Chainpoint said that his company is used for verifying records and it is very Bitcoin-friendly. They made their protocol look internal to the block chain. He stated that anything that imposes an externality on the block chain is at risk of being blocked by miners or dropped from the protocol. This means that if someone runs an inconsistent application, anchored information will be blocked from the chain in the next block. If transactions were considered external, the next change of the block chain could probably exclude them. A native solution is necessary so that the block chain and the miners can accept it on the protocol level. It is entirely possible to anchor data into the block chain in a way that causes permanent damage to the chain. However, it is also possible to do it in a way that it does not. Please refer to **Appendix C** for more details of the interview.

4.3 Interview with Robert Currie

Robert Currie is an expert in genomics and computer science. Please refer to **Appendix A** for the biography of Robert Currie and **Appendix D** for more details of the interview.

4.3.1 Benefits from block chain from a business perspective

If there were 1 billion tumor data points for tumor genomes, cancer would be revolutionized overnight. Genomics needs data. Google is running machine learning algorithms on billion images, and they are phonemically efficient. Millions of people are diagnosed with cancer every year worldwide, and a tiny percent of them go to the hospital to be sequenced, and that is creating small isolated data sets for studying. The point is how to share this data with everybody and learn from it. In the west, if someone gets cancer they will get sequenced. So, it is better to figure out how to send some of that data out, so it can flow around the world. Therefore the CGT wanted a distributed database that everyone can look on.

4.3.2 Opportunities for block chain in genomics

The ultimate goal of the CGT is to train a machine learning, a deep neural network on the DNA of every cancer patient worldwide. More specifically, the CGT wants to send their neural network training algorithm inside genomics institutions (the NKI, the University of California, Santa Cruz (UCSC), Genomics England, and others). Machine learning costs an enormous amount of computing power. A possible solution to the financial problem could be a block chain currency where the UCSC can offer the NKI, for example, 100 “genecoins” that are going to pay for mining data of a million genomes. Then the NKI could decide in a week time that they want to mine a hundred thousand genomes at Harvard Medical School and to pay Harvard; the NKI uses 10 of the genecoins the UCSC sent them. Then, Harvard can decide to send 5 of those genecoins to Genomics England just to mine data on a subset of patients who have a specific disease. The example displays a form of an economy, and there might be an incentive in mining because the CGT has created a currency, an economy for mining medical information worldwide while preserving privacy.

4.3.3 Risks in block chain for health care

A system architect has two design choices in implementing a block chain solution. The first option is to create own Genesis block and own chain – for example Genecoin, which would require for the maintainers to talk to hospitals and doctors. Doctors are not known for being the most tech savvy and comfortable, especially when there is block chain mining without incentive. The problem is how to incent people to mine. Block chains are all about incentives, and there is no incentive for a hospital to run a mining operation. The second option is to implement the idea on the Ethereum block chain or on any other viable block chain where there is already a bunch of miners. If the proposal is implemented on the Ethereum block chain and a hospital is using it, then the block chain becomes a currency for the hospital. A problem arises when the investment in ether (the currency of Ethereum) becomes worth a lot more than before, and the administrators at the hospital propose to close the hospital because they have more money than they will ever make. Another possibility could be the hospital's IT system administrator can one day realize that he or she could publish that new piece of genomics or he or she could just conveniently transfer all the ether to their account and leave to Bali.

4.3.4 Block chain as an economic opportunity in health care

To run the machine learning requires much money, and if there is a way to mediate value, to transfer value through a coin, then that becomes less of a problem. Every party can agree on price as the best way for transferring value to run the machine learning algorithms. A price allows mediating services and products regardless of what they are worldwide. So, the CGT wants to come up with an economy that is not dependent on any specific thing.

Prototype: CGT maintains their IPFS prototype on the following address: http://search.cancergenetrust.org/

4.4 Interview with Jasper Roes

Jasper Roes is involved in the block chain project of het Kadaster in the Netherlands. They are using MultiChain for their prototype, which is a permissioned block chain. Please refer to **Appendix A** for the biography of Jasper Roes and **Appendix E** for more details of the interview.

4.4.1 Benefits from using block chain for authentication

Kadaster uses the hash to ensure that they can later verify if the data is the actual data that the consumers used without having to know the data itself at that moment. Kadaster does not know the data, but they know that someone was in possession of that data at a particular time. Kadaster offers to consumers to make a hash of their data and publish it on their block chain. They can later prove the authenticity by verifying that the hash Kadaster has on the block chain is the same hash of the document.

4.4.2 Opportunities in using block chain

The main reason to look at block chain was that no one could tamper with the data. That removes the need for providing all kinds of auditing functions Kadaster would have with using databases. Block chain could offer that in one package without having to implement all sorts of processes.

4.4.3 Risks from vendor lock-in

Vendor lock-in is a significant risk in MultiChain, or it is more like a chain lock-in because it seems there is no possible way to move from one block chain to another. Block chains are not interoperable. Kadaster is not very fond of this fact. By choosing MultiChain, they are not able to move to any other chain. Another risk is that it is still very early, so many solutions have to prove themselves. Kadaster needs to find whether those solutions can, in the end, handle the things they need them to do.

Prototype: Kadaster has published their prototype at the following address: http://www.eenvoudigbeterbouwen.nl/

4.5 Interview with Maarten Everts

Maarten Everts is an expert in cryptography and specialist in block chain technologies. Please refer to **Appendix A** for the biography of Maarten Everts and **Appendix F** for more details of the interview.

4.5.1 Benefits rely on people's collaboration

Block chains work if there is collaboration. Collaboration on own is silly because having one node is just the same as having a server in the basement. The benefits from using block chains come from enough people using it and from mass acceptance.

A block chain could help people with arbitrary decisions. It is a useful tool for checking history because it is considerably harder to compromise its records than traditional ledger systems.

4.5.2 Opportunities in suppressed countries

Block chains can be especially useful in helping suppressed countries with corrupt governments where there is a lack of regulation. If there are enough people to accept block chain as a technology to trust, it can be turned into means for creating proofs for decision-making about ownership and truth.

4.5.3 Risks to privacy in public block chains

Most significant risks for public (permissionless) block chains is the lack of privacy. Everything is public, nothing is hidden, and that data is traceable and pseudo-anonymous. Users depend on something that is public.

4.5.4 Block chains are hype

Most of the reason why there is so much interest in block chains is FOMO (Fear of missing out) and hype. Most of the problems companies are trying to solve with block chain are usually easily solved with simpler solutions, more efficiently. The block chain mania is significantly similar to the internet explosion in the 90s.

4.6 Interview with Stephen Wilson

Stephen Wilson is critical of block chains. Please refer to **Appendix A** for the biography of Stephen Wilson and **Appendix G** for more details of the interview.

4.6.1 Opportunities for private block chains

Mr. Wilson is a believer in the Hyperledger initiative for building private (permissioned) block chain-based DLTs for business applications.

Topics	Summary of findings
Private block chain use cases	1. Complex multi-party financial transactions 2. Trade & shipping manifests 3. Supply chain 4. Trade finance
No need for decentralization	Decentralization ≠ Security. For private block chains, different security models are applied to maintain the immutability of the ledger.
Private vs. Public regarding security	In private block chain, the focus is on the security of the nodes, whereas in public block chains the security of the nodes does not matter because the swarm takes care of rogue players.

Mr. Wilson concludes that the properties of the original block chain were entirely designed only to prevent double spending. The properties of Bitcoin's block chain – "immutability, decentralization, transparency, freedom, and trustlessness – came tightly bundled, expressly to run peer-to-peer cryptocurrency." Recently, he coined a new term – "Synchronous Ledger Technologies" (SLT) which is a block chain spinoff to describe a more accurate explanation of new superior infrastructures beyond block chains designed "to orchestrate agreement on some property of a complex set of transaction data" (Wilson, 2017c, "Why Synchronous Ledger Technology").

4.6.2 Risks from technological limitations

Mr. Wilson makes a distinction between block chain and more advanced ledger technologies. What he calls first generation block chains are the public block chains like Bitcoin and Ethereum. Most of the significant impediments are listed in the table. However, it is probably not appropriate to characterize newer more advanced ledger technologies as “blocked” by technological problems, because they are all works in progress and not yet released for use.

Topics	Summary of findings
Impediments for public block chains	1. Performance limitations 2. Technical indecision around critical software specifications like block size 3. The specter of hard forks as a brutal way of breaking through design deadlocks 4. Poor key management

4.6.3 Risks from implementation in health care

Mr. Wilson states that public block chains have no application for HIEs. Other more advanced ledger technologies might have a better purpose, but they must have first a clear explanation of the problems they would solve. Block chain was created for a particular use case that is utterly unlike health care. HIE is a fiercely complicated problem. The core idea of ledger technologies is disintermediation and consensus in multi-party environments with little or no leadership, which raises the question whether health care is like that.

4.7 Interview with Christopher DeRose

Christopher DeRose is a Bitcoin evangelist developer and journalist. He is hosting a show on YouTube called “Bitcoin Uncensored.” Please refer to **Appendix A** for the biography of Christopher DeRose and **Appendix H** for more details of the interview.

4.7.1 Benefits from running a block chain

Censorship-resistance is the number one reason why someone would bother to run thousands of computers around the world consuming massive amounts of electricity, and the need to convert registered value (electricity) into anonymous value for payment processing.

4.7.2 Risks from volatility, user experience, and transparency

The instability of the price of the coins is one of the most significant risks in using a public block chain. Another risk factor is the user interface issues caused by push-based systems without reversibility (stolen/lost keys). Data transparency is also a risk for users. If medical data is stored in the block chain, then it will be shared with all members of the block chain which poses a security risk.

4.7.3 Misleading reasons for implementing block chain

Some of the factors that drive organizations to believe they need a block chain are 1) technically inept managers who control the R&D funding by looking to attach a buzzword to their R&D goals. Another example is 2) managers that hold cryptocurrencies, and who are looking (through willful ignorance or otherwise) to increase the value of their investment position further. A good example for this was a power company that wanted to build Ethereum charging stations in Germany. One of the chief persons involved was an ether holder. Finally, 3) some managers are looking to add a competency to their resume, in an industry that they perceive as promising.

4.7.4 Impediments in implementation

Mr. DeRose states that the current progress on implementing block chain in businesses is at the stage of building a lot of coalitions and standards bodies, where nothing is achieved but whiteboarding the dreams of its members.

4.8 Interview with Erich Erstu

Erich Erstu is a developer and owner of a time-stamping service on the Bitcoin's block chain called "Cryptograffiti.info ." Please refer to **Appendix A** for the biography of Erich Erstu and **Appendix I** for more details of the interview.

4.8.1 Opportunities in storing data into the block chain

Mr. Erstu says that couples like to use his service to post photos and devotion messages on the block chain. Others use it for time-stamping their files. People from heavily censored countries have also written some political messages on the block chain using cryptograffiti.info.

4.8.2 Benefits from using block chain for records

Cryptograffiti only stores the IP addresses of users who use the message encoding service to store their custom data on the block chain. Also, Cryptograffiti only stores the transaction hashes on their database, so the data itself is kept on the Bitcoin's block chain. The bitcoin network maintains the data integrity.

4.8.3 Risks

The most prominent risks in using block chain are that most of the time the problem someone is trying to solve with a block chain does not need a block chain in the first place.

4.8.4 Measuring progress

A reliable way to gauge the success of a block chain notary would be winning the first court case thanks to a time-stamp on a block chain. Then the concept of a trustless notary service has succeeded. Most likely, many lawyers specializing in the notary business and patenting will have to find another job.

4.9 Interview with Jaco van de Pol

Jaco van de Pol is a professor of Computer Science at the University of Twente. Please refer to **Appendix A** for the biography of Jaco van de Pol and **Appendix J** for more details of the interview.

4.9.1 Benefits and reasons to use a block chain

Dr. van de Pol states some of the reasons he thinks why banks embrace block chain, and which also partly spreads over to other domains. 1) Fear of missing out: if banks might become obsolete, there is a good chance to lead the successor technology. 2) International trading through various legal systems is difficult. 3) No overhead from intermediate actors or supervisors with using block chain. 4) It provides some level of privacy (probably debatable). 5) It allows secure exchange of information without a TTP.

4.9.2 General risks

Topics	Summary of findings
Risks	1. Partners want to drop out from the system 2. The technology provider disrupts the service 3. Vendor lock-in 4. Other risks, like the crypto is broken, the system is hacked 5. Misunderstanding by users 6. Overselling by technicians 7. Attacks on technical infrastructure 8. Leak of crucial information

4.9.3 Technological risks, barriers, and impediments

Mainly, 1) the PoW concept is costly and costs much energy. People try to move away from it, e.g., by PoS. As a consequence, the throughput of the network (max number of transactions per second) is insufficient for large-scale applications. 2) People are technically uncertain whether to run a block chain or which service to use. 3) Furthermore, people might be afraid that they might lose their electronic wallet or that someone steals it. 4) Smart contracts are “executable code” that “codifies” the agreement between actors. These contracts also end up in the block chain, so they are irrevocable. If a contract is faulty, it cannot be fixed once in the block chain.

4.9.4 Unclear opportunities

It is often an overkill when people speculate on what block chain can do. The BGP is a hard problem, which requires many resources. If there is some trust among the parties, or if a central authority is acceptable, these are much more efficient solutions.

Trusting a TTP on a block chain can be an issue, but a small one. However, if the block chain is sufficiently large, there is no real ‘provider.' It could run as an open source project. Although, even Facebook, Google - the “free” and open internet, became subject to some monopolists, so that might happen with block chain as well.

4.9.5 Block chain hype

The required level of confidentiality in health care and legal record keeping is very high, so that would be the main focus at first. Another issue is to look for current models that might solve problems more efficiently. Would it be possible to address the problem with existing technologies and does it result in improvement?
Block chain is hype, and we do not know what is possible. There is just a burst of creativity of potential applications. It is a good learning curve.

4.10 Interview with Maqsood Ahmed

Maqsood Ahmed is Technical Fellow at PACCAR INC – a Fortune 500 truck manufacturing company. They are interested in block chain implementation. Please refer to **Appendix A** for the biography of Maqsood Ahmed.

4.10.1 Benefits from a transparent and ordered list

One of the main advantages of a block chain is that it offers the possibility of having an ordered data structure that cannot be altered and that can be traced because it is transparent. Others benefits are visibility, reliability, and accountability to make sure the product delivered at the end of the supply chain is auditable and fulfills the need of the organization.

4.10.2 Opportunities in ordering and reporting

So far PACCAR is not looking for block chain to fix problems but to enhance the existing and new processes and make them more efficient.

There are many opportunities for improving several current processes they have by utilizing block chain technology. For example, ordering truck parts, leasing trucks, reporting on when a truck is due for maintenance.

4.10.3 Risks in relying on outside actors

The security risk is the first one that comes to mind. So far, they have not heard of any security breach, but relying on external vendors with different technologies which are an overall part of the block chain may create security risks.

4.10.4 Real use cases and management sponsorship

Management sponsorship and practical use cases are the most significant factors to kick off a block chain initiative. Mr. Ahmed thinks that a block chain initiative is something both technology and business teams have to decide. The technology team would not want to introduce a solution that is something business teams do not seem to have any interest or desire. Successful implementation of block chain has to be a mutual goal.

4.11 Analysis

Statement pro	Statement against	Verdict and arguments
Block chains allow for maintaining a tamper-proof ordered data structure, which removes the need to audit data and operations.	An ordered list is only necessary for individual cases. If there is no need for an ordered list, then there is no use for a block chain.	Financial services must have an ordered list and so are supply chains. An ordered list is not a necessity for health care. Therefore, a block chain would add unnecessary complexity.
Block chains operate without a central authority.	Central authority and administration are of high importance in specific industries.	In health care, it is vital to know who is who and trust is a requirement. Block chain's primary purpose was to avoid TTP. Ledger technologies do no provide trust.

Block chains provide privacy and provenance.	Public-key cryptography also gives privacy and provenance.	Institutions can de-identify data of patients for analysis. Particularly useful in machine learning. However, institutions need to know who is who in the data exchange among one another. Public-key cryptography is enough to prove data ownership in data exchange because institutions have created an off-chain trust. There is no need for miners nor block chains.
Block chains can create economies.	There should be a good reason to create an economy.	Creating a private economy could be advantageous for a specialized use case. The currency can be a medium of exchange for mining big data (the currency is backed by data). This currency can only be used in the private environment and not outside (e.g., a permissioned block chain with a token that can only be exchanged for data).
Block chains are useful, efficient and can protect information from fraud in organizations and it is harder to compromise.	The protection block chains offer comes at a cost. They consume vast amounts of energy, and there is no way to reverse stolen or lost keys. Also, data is transparent and public which can be a problem if storing private information.	Block chains need to solve the critical issues with its interoperability, vendor-lock ins, and key management. It still immature technology and if someone loses their keys all of their data is gone forever. A person can restore a lost ID, but he or she cannot restore a lost private key.
Block chains can certify the authenticity and ownership of documents. Data is immutable and time-stamped	Identity cannot be verified on a trustless block chain by just verifying the signature.	The problem with identity on the block chain is unsolved. A digital signature does not prove identity. It only proves ownership of a hash on the chain. An off-chain trust is necessary to prove identity, similar to a regular notary (Kadaster).

5 Discussion and Conclusion

The purpose of the study was to build a conclusion whether block chains are useful in dealing with patients' data, anchoring data, and just in general whether they are a good choice for other areas beyond use cases for payments. More specifically, the research question wanted to know the probable outcomes from block chain implementation in health care and legal record keeping. The research methods required an analysis of the theory, and an analysis of the interviews with experts. The findings showed that much more experiments and testing should be conducted on block chains. There are not many chains or ledger technologies to work with, and most of the projects are still in very early stages of development. This study is designed to contribute to the research on alternative uses cases for block chains. During the research, it was found that there were some inconsistencies in the literature, for example, the claim that block chains create trust when it is precisely the opposite. Block chains remove the need for trust.

The purpose of creating the first block chain was to prevent double spending and the creation of a digital bearer asset. It can be even argued that the block chain is an "artifact which is the best current way to implement bearer" (Back, 2017). It was initially designed for transferring electronic money over the internet. The creation of the block chain was one directional proposition - to prevent double spend in e-cash and to facilitate currency transactions. The properties of the first block chain – immutability, decentralization, transparency, trustlessness – are designed to run peer-to-peer cryptocurrency. However, much more complex systems have emerged from that in the field of permissioned block chains designed to accompany business functions. Those functions are yet to be seen in a real-world use case.

Based on the results of interviews and the analysis there is little to be excited for block chains outside of value transfer. The outlook looks vague for the most part. A compelling use case is the Cancer Gene Trust idea to create a private economy for mining genomic data to create a neural network but that is yet to be seen how successful it would turn out.

Private block chains seem more plausible for business use cases. They are faster, permissioned and centralized. Where administration is necessary, private block chains are more logical to use. Public block chains are risky and volatile to be applied in health care or notary. There is much uncertainty in public block chains. Maarten Everts said public block chains are interesting test bench.

The best thing to do is wait for something viable to come out from the permissioned block chains (Hyperledger, Corda). At the moment the only usefulness of a block chain is in creating a currency and nothing else. More complex use cases could come after introducing other technological layers that make use of public block chains, or by connecting private block chains to public chains. In a trustless public block chain, it is hard to build a use case where trust is a must. The third parties are the machines, the miners in public block chains and no one can control them on the protocol level.

The study can be used as a contribution to the paper of Wüst & Gervais (2017) "*Do you need a Blockchain?*" or other papers which discuss block chain types in different use cases. Adopting a block chain should be based on the application of the specific use case. The choice between permissioned or permissionless block chain should be determined according to the use case.

What are the probable outcomes for block chain implementation in health care and legal record keeping?"

A possibility for block chain in health care is to wait for a solution from IBM, Deloitte or others that are pushing R&D in that direction. Those companies have teams working on designing permissioned solutions for health care. The public block chains are not suited for health care. Operations on public block chains are slow and pose many risks, for example accessing someone's private data because it was stored on a publicly accessible structure. In health care, key management is the biggest and most important issue to solve. That problem needs to be dealt with, otherwise storing private data guarded by a key is not going to work. Both legal record keeping and health care require an off-chain trust and a proper identity to function.

1. What factors drive organizations believe they need block chain?

Key factors driving organizations into block chain is the hype and money that is poured into the development of projects. Similar to the dot-com bubble things will have their explosive moment, and a big part of those projects might close down. Some managers are misguided. They read the marketing materials and press releases of block chains and ICO projects, and because of the amount of money being invested, those managers assume this technology could be promising. Most of the promises for fixing and optimizing operations and disrupting industries are highly probable to be vaporware. There are no real barriers for anyone to create a block chain and sell it to the public.

2. What are the current technological impediments blocking block chain implementation?

Standards. Block chains are not interoperable, and they are not compatible with anything else. Switching from one system to another is not easy, and in the case of health care, it is very complex because of the deep levels of infrastructure there. If block chains are to transform and disrupt industries and bring revolution, then there will be many barriers to be dealing with: technological, governance, organizational, and even societal. At the moment not much is done on those issues. Governments are still somewhat indifferent about block chains. Current progress on legislation is still mostly oriented towards cryptocurrencies.

3. What is the current progress on block chain implementation?

Mostly whiteboarding and forming standard bodies. No real business application is yet seen apart from cryptocurrencies. First big implementations to be expected will be in the financial services probably in the form of a stock exchange which would offer lower costs for transacting.

4. What are the overall costs for a block chain implementation?

Public block chains are easier to quantify because their operational data is publically available. However private block chains are still a mystery. For example, time-stamping a document on a public block chain is relatively cheap, ~€5 per document. Costs are unclear for now which makes it even harder to predict future scenarios after potential implementation.

5. What are possible developments after implementation?

After implementation, it would be wise to convince others to start accepting the block chain standard and more importantly to convince governments to accredit it. At the moment there are small regulatory developments for block chains. If block chains are indeed necessary for society, they will need to have a clear regulatory climate, especially if used in health care, legal records and permits. The immaturity of the technology makes it hard to predict how would organizations measure development.

6. How would organizations measure progress and efficiency of a block chain?

Measuring transparency of data, trust or censorship-resistance on a block chain is difficult because they are subjective values. However, dollars saved relative to costs incurred would be an appropriate measurement tool. Also, the frequency of censorship attempts on the chain is another interesting measurement. The lower transaction costs and people using it are reliable benchmarks as well.

Some of the limitations of this research were the lack of data because not many are using block chains outside of payments and also the time constraints for completing the research. This topic can potentially be expanded by including permissioned block chains (so-called DLTs). The general verdict of the study can also be applied in other non-monetary use cases.

This research can be expanded by studying DLTs (or also now known as SLTs) which are expected to be more suitable for enterprise implementations. With the upcoming releases of Hyperledger Fabric and R3 Corda and their potential future implementations, it would be interesting to study how these new types of block chain based technologies can adapt to health care, legal record keeping and other valuable areas such as banking, derivatives, identity. For public block chains, there are upcoming scaling solutions which could potentially create many new use cases. All the future scaling solutions for Bitcoin are also very interesting - Side chains, Lightning network, TumbleBit. The upcoming Merkelized Abstract Syntax Trees (MAST) addition on Bitcoin is also fascinating. It would allow smaller and more private transactions, and also would allow for more sophisticated smart contracts. PoWs are considered wasteful in some regard because of burning electrical energy to secure the block chain. New experimental consensus ideas to remove waste such as “proofs of space and time,” by Bram Cohen, creator of BitTorrent and also “proof of useful work” seem like good ideas for research. They could bring a very positive impact if studied further.

6 References

Journals, articles, reports, and books

Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Inc.

Barbieri, M., & Gassen, D. D. (2017). Blockchain – can this new technology really revolutionize the land registry system? In *Land and Poverty Conference 2017: Responsible Land Governance*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-app-in-public-sector.pdf

Bastiaan, M. (2015). Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin. In *22nd Twente student Conference on IT* (pp. 1–10).

Beltran-Aroca, C. M., Girela-Lopez, E., Collazo-Chao, E., Montero-Pérez-Barquero, M., & Muñoz-Villanueva, M. C. (2016). Confidentiality breaches in clinical practice: what happens in hospitals? *BMC Medical Ethics*, *17*(1), 52. https://doi.org/10.1186/s12910-016-0136-y

BitFury Group. (2016). *Digital Assets on Public Blockchains* (Vol. 2016).

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. In *IEEE Symposium on Security and Privacy* (Vol. 2015–July, pp. 104–121). https://doi.org/10.1109/SP.2015.14

Bradbury, D. (2013). The problem with Bitcoin. *Computer Fraud and Security*, *2013*(11), 5–8. https://doi.org/10.1016/S1361-3723(13)70101-5

Buldas, A., Kroonmaa, A., & Laanoja, R. (2013). Keyless signatures' infrastructure: How to build global distributed hash-trees. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 8208 LNCS, pp. 313–320). https://doi.org/10.1007/978-3-642-41488-6_21

Burniske, C. (Ark I., & White, A. (Coinbase). (2017). *Bitcoin: ringing the bell for a new asset class*.

Choucri, N., & Clark, D. D. (2012). *Integrating Cyberspace and International Relations: The Co-Evolution Dilemma* (No. 2012–29). *MIT Political Science Department Research Paper No. 2012-29*. https://doi.org/10.2139/ssrn.2178586

Christin, N. (2012). *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*. https://doi.org/10.1145/2488388.2488408

Ciaian, P., Rajcaniova, M., & Kancs, D. (2016). The digital agenda of virtual currencies: Can BitCoin become a global currency? *Information Systems and E-Business Management*, *14*(4), 883–919. https://doi.org/10.1007/s10257-016-0304-0

De Nederlandsche Bank N.V. (2016). *2016 Annual Report*. https://doi.org/10.1039/C1DT90165F

European Union Agency for Network and Information Security. (2016). *Distributed Ledger Technology & Cybersecurity Improving*.

Eyal, I., & Sirer, E. G. (2014). Majority is not Enough: Bitcoin Mining is Vulnerable. In *International conference on financial cryptography and data security* (pp. 436–454). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-45472-5_28

Figurska, M., Stańczyk, M., & Kulesza, K. (2008). Humans cannot consciously generate random numbers sequences: Polemic study. *Medical Hypotheses*, *70*(1), 182–185. https://doi.org/10.1016/j.mehy.2007.06.038

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the Security and Performance of Proof of Work Blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16* (pp. 3–16). ACM. https://doi.org/10.1145/2976749.2978341

Giaglis, G. M., & Kypriotaki, K. N. (2014). Towards an Agenda for Information Systems Research on Digital Currencies and Bitcoin. *Business Information Systems Workshops, 183*, 3–13. https://doi.org/10.1007/978-3-319-11460-6_1

Gipp, B., Meuschke, N., & Gernandt, A. (2015). Decentralized Trusted Timestamping using the Crypto Currency Bitcoin. *iConference 2015,* 1–6. Retrieved from http://arxiv.org/pdf/1502.04015v1

Haber, S., & Stornetta, W. S. (1990). How to Time-Stamp a Digital Document. *Advances in Cryptology-CRYPT0' 90*, 437–455. https://doi.org/10.1007/3-540-38424-3_32

Karame, G. O., Androulaki, E., & Capkun, S. (2012). Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. *IACR Cryptology ePrint Archive*, *2012*(248).

Krawiec, R., Housman, D., White, M., Filipova, M., Quarre, F., Barr, D., … Tsai, L. (2016). Blockchain: Opportunities for Health Care. In *NIST Workshop Blockchain Healthcare (Deloitte)* (pp. 1–16).

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems (TOPLAS), 4*(3), 382–401.

Laurent, A. M. S. (2004). *Understanding Open Source and Free Software Licensing: Guide to Navigating Licensing Issues in Existing & New Software*. O'Reilly Media Inc. Retrieved from https://books.google.nl/books?id=04jG7TTLujoC

Lin, I.-C., & Liao, T.-C. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, *19*(5), 653–659. https://doi.org/10.6633/IJNS.201709.19(5).01

Lindman, J., Rossi, M., & Tuunainen, V. K. (2017). Opportunities and risks of Blockchain Technologies in payments – a research agenda. In *50th Hawaii International Conference on System Sciences (HICSS 2017)* (pp. 1533–1542).

Maxwell, J. A. (2008). Designing a Qualitative Study. In *The SAGE Handbook of Applied Social Research Methods* (pp. 214–253). SAGE Publications, Inc. https://doi.org/10.4135/9781483348858.n7

Merkle, R. C. (1982). Method of Providing Digital Signatures. *US Patent 4,309,569*. Washington, DC: U.S. Patent and Trademark Office. Retrieved from https://www.google.com/patents/US4309569

Merkle, R. C. (1989). Digital signature system and method based on a conventional encryption function. *US Patent 4,881,264*. Washington, DC: U.S. Patent and Trademark Office. https://doi.org/10.1007/3-540-48184-2_32

Merkle, R. C. (1990). A certified digital signature. In *Advances in Cryptology—CRYPTO'89 Proceedings* (pp. 218–238). Springer Berlin Heidelberg. https://doi.org/10.1007/0-387-34805-0_21

Miller, A., & LaViola, J. J. (2014). *Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin*. *Computer Science-Tech Report*. Retrieved from http://nakamotoinstitute.org/static/docs/anonymous-byzantine-consensus.pdf

Möser, M., Böhme, R., & Breuker, D. (2014). Towards Risk Scoring of Bitcoin Transactions. In R. Böhme, M. Brenner, T. Moore, & M. Smith (Eds.), *Financial Cryptography and Data Security: FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers* (pp. 16–32). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-44774-1_2

Nakamoto, S. (2008a). Bitcoin: A Peer-to-Peer Electronic Cash System. *Www.Bitcoin.Org*, 9. https://doi.org/10.1007/s10838-008-9062-0

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press. Retrieved from http://www.the-blockchain.com/docs/Princeton Bitcoin and Cryptocurrency Technologies Course.pdf

Narayanan, A., & Clark, J. (2017). Bitcoin's Academic Pedigree. *ACM Queue*, *15*(4), 1–30. https://doi.org/10.1145/3134434.3136559

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183–187. https://doi.org/10.1007/s12599-017-0467-3

Nomura Research Institute. (2015). *Survey on Blockchain Technologies and Related Services*. *Nomura Research Institute & Japan's Ministry of Economy, Trade and Industry (METI)*.

Ozisik, A. P., & Levine, B. N. (2017). An Explanation of Nakamoto's Analysis of Double-spend Attacks. *arXiv Preprint arXiv:1701.03977*, 1–15.

Patterson, S. (2015). *What's the Big Deal About Bitcoin?* Retrieved from http://steve-patterson.com/wp-content/uploads/2015/03/WhatsTheBigDealAboutBitcoin.pdf

Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. *Technical Report (Draft)*, 59. Retrieved from https://lightning.network/lightning-network-paper.pdf

Rauchs, M., & Hileman, G. (2017). Global Cryptocurrency Benchmarking Study. *Cambridge Centre for Alternative Finance*.

Rijnbout, J. (2017). Byzantine Consensus Through Bitcoin's Proof-of-Work. *Management Control & Accounting*, (1), 40–44.

Robla, E. S. (2015). *Analysis of Reward Strategy and Transaction Selection in Bitcoin Block Generation*. (Doctoral dissertation). University of Washington Libraries. Retrieved from https://digital.lib.washington.edu/researchworks/bitstream/handle/1773/33802/SenmartiRobla_washington_0250O_14491.pdf?sequence=1&isAllowed=y

Schneider, J., Blostein, A., Lee, B., Kent, S., Groer, I., & Beardsley, E. (2016). Goldman Sachs Equity Research Profiles in Innovation. *Blockchain Putting Theory into Practice*.

Shelkovnikov, A. (2016). Blockchain applications in the public sector. *Deloitte*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-app-in-public-sector.pdf

Solum, L., & Chung, M. (2004). The Layers Principle: Internet Architecture and the Law. *Notre Dame Law Review*, *79*(3), 815–948. https://doi.org/10.2139/ssrn.416263

Tasca, P. (2015). *Digital Currencies: Principles, Trends, Opportunities, and Risks*. *Deutsche Bundesbank and ECUREX Research*. https://doi.org/http://dx.doi.org/10.2139/ssrn.2657598

the Economist. (2015). The trust machine | The Economist. *The Economist*, p13,p23-26. Retrieved from http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

Tierion. (2016). *Blockchain Healthcare Promise & Pitfals*.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys & Tutorials*, *18*(3), 2084–2123. https://doi.org/doi: 10.1109/COMST.2016.2535718

Visa. (2015). *Visa Inc. at a Glance*. Retrieved from https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf

Wilson, S. (2016a). *Beyond the Hype: Understanding the Weak Links in the Blockchain*.

Wilson, S. (2017a). *Blockchain Explained in Plain English*.

Wilson, S., & Chou, D. (2017). How Healthy is Blockchain Technology? In *HIMSS AsiaPac17* (pp. 1–10).

Wüst, K., & Gervais, A. (2017). *Do you need a Blockchain? Cryptology ePrint Archive (International Association for Cryptologic Research)*.

Yee, A. (2014). Internet architecture and the layers principle: a conceptual framework for regulating Bitcoin. *Internet Policy Review*, *3*(3), 1–9. https://doi.org/10.14763/2014.3.289

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), 1–27. https://doi.org/10.1371/journal.pone.0163477

Websites

Antonopoulos, A. (2014). *Bitcoin security model: trust by computation*. Retrieved from O'Reilly Media: http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html

Back, A. (2017). *Twitter*. Retrieved from Twitter: https://twitter.com/adam3us/status/910545422002933761

Bitcoin Uncensored. (2017). *Nicholas Dorier talks Mimble Wimble, Lightning, Tokyo, and .NET Bitcoin programming*. Retrieved from YouTube: https://www.youtube.com/watch?v=Kf_WM0LxLEs&feature=youtu.be&t=35m25s

Bitcoin Wiki. (2016a). *Bit Gold proposal*. Retrieved from Bitcoin Wiki: https://en.bitcoin.it/wiki/Bit_Gold_proposal

Bitcoin Wiki. (2016b). *Block*. Retrieved from Bitcoin Wiki: https://en.bitcoin.it/wiki/Block

Bitcoin Wiki. (2016c). *Off-Chain Transactions*. Retrieved from Bitcoin Wiki: https://en.bitcoin.it/wiki/Off-Chain_Transactions

Bitcoin Wiki. (2017a). *Confirmation*. Retrieved from Bitcoin Wiki: https://en.bitcoin.it/wiki/Confirmation

Bitcoin Wiki. (2017b). *Contract*. Retrieved from Bitcoin Wiki: https://en.bitcoin.it/wiki/Contract

Bitcoin Wiki. (2017c). *Multisignature*. Retrieved from Bitcoin Wiki: https://en.bitcoin.it/wiki/Multisignature

Bitcoin Wiki. (2017d). *OP_RETURN*. Retrieved from Bitcoin Wiki: https://en.bitcoin.it/wiki/OP_RETURN

Bitcoin Wiki. (2017e). *Private key*. Retrieved from Bitcoin Wiki: https://en.bitcoin.it/wiki/Private_key

BitLegal. (2017). *BitLegal World Map*. Retrieved from BitLegal: http://bitlegal.io/

Bitsonblocks. (2016). *"Why do miners mine?"*. Retrieved from Bitsonblocks: https://bitsonblocks.net/2015/09/21/a-gentle-introduction-to-bitcoin-mining/

Blockchain.info. (2017). *Pools*. Retrieved from Blockchain.info: https://blockchain.info/pools?timespan=4days

Cheliak, B. (2016). *How the Technology Behind Bitcoin Could Provide a Tech Revolution for the Fire Service.* Retrieved from DCEBrief: https://dcebrief.com/how-the-technology-behind-bitcoin-could-provide-a-tech-revolution-for-the-fire-service/

Greenberg, A. (2011). *WikiLeaks Asks For Anonymous Bitcoin Donations*. Retrieved from Forbes Media: https://www.forbes.com/sites/andygreenberg/2011/06/14/wikileaks-asks-for-anonymous-bitcoin-donations/#36f4f03c4f73

Hertig, A. (2017). *Julian Assange Just Read Out a Bitcoin Block Hash to Prove He Was Alive*. Retrieved from Coindesk: http://www.coindesk.com/julian-assange-just-read-bitcoin-block-hash-prove-alive

Higgins, S. (2016). *40 Banks Trial Commercial Paper Trading in Latest R3 Blockchain Test*. Retrieved from Coindesk: https://www.coindesk.com/r3-consortium-banks-blockchain-solutions/

Investopedia. (2017). *Bearer Instrument*. Retrieved from Investopedia: http://www.investopedia.com/terms/d/definitive-securities.asp

Investor.gov. (2017). *Investor Bulleting: Initial Ccoin Offerings*. Retrieved from Investor.gov: https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings

Jefferson Lab. (n.d.). *How many atoms are in the human body?* Retrieved from Jefferson Lab: http://education.jlab.org/qa/mathatom_04.html

livegnik. (2016). *BitCoin-v0.01-ALPHA*. Retrieved from GitHub: https://github.com/livegnik/BitCoin-v0.01-ALPHA/blob/master/src/main.h#L795

Merriam-Webster. (n.d.-a). *after-the-fact*. Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/after-the-fact

Merriam-Webster. (n.d.-b). *incorruptible*. Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/incorruptible

Microsoft. (2017). *TCP/IP Protocol Architecture*. Retrieved from Microsoft: https://technet.microsoft.com/en-us/library/cc958821.aspx

Monegro, J., Wilson, F., Wenger, A., & Ali, M. (2014). *The Blockchain Application Stack*. Retrieved from Joel: http://joel.mn/post/103546215249/the-blockchain-application-stack

Nakamoto, S. (2008b). *Re: Bitcoin P2P e-cash paper*. Retrieved from The Mail Archive: http://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html

O’Leary, M. (2016). *The Mysterious Disappearance of Satoshi Nakamoto, Founder & Creator of Bitcoin*. Retrieved from Huffingtonpost: http://www.huffingtonpost.com/martin-oaleary/the-mysterious-disappeara_2_b_7217206.html

O'Leary, R. R. (2017). *Russia's Central Bank Backs Move to Block Bitcoin Websites*. Retrieved from Coindesk: https://www.coindesk.com/russias-central-bank-backs-move-to-block-bitcoin-websites/

OP_RETURN Stats. (n.d.). *OP_RETURN Stats*. Retrieved from OP_RETURN Stats: http://opreturn.org/

Ou, E. (2016). *Maybe Blockchain Really Does Have Magical Powers*. Retrieved from Bloomberg: https://www.bloomberg.com/view/articles/2016-09-01/maybe-blockchain-really-does-have-magical-powers

Oxford Dictionaries. (2017). *vaporware*. Retrieved from Oxford Dictionaries: https://en.oxforddictionaries.com/definition/us/vaporware

Peck, M. (2015). *Adam Back Says the Bitcoin Fork Is a Coup*. Retrieved from IEEE: http://spectrum.ieee.org/tech-talk/computing/networks/the-bitcoin-for-is-a-coup

Perez, Y. B. (2015). *Santander: Blockchain Tech Can Save Banks $20 Billion a Year*. Retrieved from Coindesk: https://www.coindesk.com/santander-blockchain-tech-can-save-banks-20-billion-a-year/

Peters, A. (2016). *Tracking Tuna On The Blockchain To Prevent Slavery And Overfishing*. Retrieved from Fast Company: https://www.fastcompany.com/3063440/tracking-tuna-on-the-blockchain-to-prevent-slavery-and-overfishing

PSBlake. (2014). *On the subject of listing all possible Private Keys...* Retrieved from Reddit/r/Bitcoin: https://www.reddit.com/r/Bitcoin/comments/1rurll/on_the_subject_of_listing_all_possible_private/

satoshi. (2010). *They want to delete the Wikipedia article*. Retrieved from Bitcointalk: https://bitcointalk.org/index.php?topic=342.msg4508#msg4508

Stark, E. (2017). *Elizabeth Stark of Lightning Labs: "The Importance of Layer Two" | Blockstack Summit 2017*. Retrieved from YouTube: https://www.youtube.com/watch?v=3PcR4HWJnkY

Sullivan, N. (2013). *A (relatively easy to understand) primer on elliptic curve cryptography*. Retrieved from Arstechnica: https://arstechnica.com/information-technology/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

Szabo, N. (1996). *Smart Contracts: Building Blocks for Digital Markets*. Retrieved from Phonetic Sciences, Amsterdam: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Szabo, N. (2011). *Bitcoin, what took ye so long?* Retrieved from Unenumerated: https://unenumerated.blogspot.nl/2011/05/bitcoin-what-took-ye-so-long.html

Sztorc, P. (2016). *BTC Codex - The Digital Identity Sidechain*. Retrieved from Truthcoin: http://www.truthcoin.info/blog/codex-identity-sidechain/#trustless-buying-of-identify-verification-offchain

Sztorc, P. (2017). *Two Types of Blockspace Demand*. Retrieved from Truthcoin: http://www.truthcoin.info/blog/blockspace-demand/

The BBC. (2010). *Wikileaks: Swiss bank shuts Julian Assange's account*. Retrieved from The BBC: http://www.bbc.com/news/world-11929034

Tian, C. (2017). *$1.6 Billion: All-Time ICO Funding Climbs as Record $500 Million Invested in July*. Retrieved from Coindesk: https://www.coindesk.com/1-6-billion-all-time-ico-funding-climbs-as-record-500-million-invested-in-july/

Todd, P. (2014). *PayPub: Trustless payments for information publishing on Bitcoin*. Retrieved from Github: https://github.com/unsystem/paypub

Torpey, K. (2016). *Eric Lombrozo: Bitcoin Needs Protocol Layers Similar to the Internet*. Retrieved from Coinjournal: https://coinjournal.net/eric-lombrozo-bitcoin-needs-protocol-layers-similar-to-the-internet/

U.S. Department of Health & Human Services. (2015). *The HIPAA Privacy Rule*. Retrieved from U.S. Department of Health & Human Services: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

U.S. Department of Health & Human Services. (2017). *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. Retrieved from U.S. Department of Health and Human Services: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

vamsital. (2016). *The Architecture of Blockchain*. Retrieved from Vamsi Talks Tech: http://www.vamsitalkstech.com/?p=1615

Versteegh, B. (2014). *Bitcoin Cheatsheet*. Retrieved from Github: https://github.com/boukeversteegh/bitcoin-cheatsheet

Villanueva, J. C. (2015). *How Many Atoms are there in the Universe?* Retrieved from Universe Today: https://www.universetoday.com/36302/atoms-in-the-universe/

Waterman, S. (2016). *Web consortium weighs work on blockchain standards*. Retrieved from FedScoop: https://www.fedscoop.com/web-consortium-starts-work-on-blockchain-standards/

Wikipedia. (2017a). *Bit*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Bit#cite_note-Mackenzie_1980-1

Wikipedia. (2017b). *Diffie–Hellman key exchange*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#cite_note-1

Wikipedia. (2017c). *Ethereum*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Ethereum

Wikipedia. (2017d). *Elliptic-curve cryptography*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

Wikipedia. (2017e). *Nick Szabo*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Nick_Szabo#cite_note-PeckBitcoin2012-9

Wikipedia. (2017f). *Prisoner's dilemma*. Retrieved from Wikimedia: https://en.wikipedia.org/wiki/Prisoner%27s_dilemma

Wikipedia. (2017g). *RSA (cryptosystem)*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

Wikipedia. (2017h). *Silk Road (marketplace)*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Silk_Road_(marketplace)

Williams-Grut, O. (2016). *Blockchain startup R3 is raising $200 million from big banks — but one of them is 'throwing stones'*. Retrieved from Business Insider:

http://uk.businessinsider.com/blockchain-r3-raising-money-big-banks-pushback-2016-5?international=true&r=UK&IR=T

Williams-Grut, O. (2017). *GOLDMAN: 'It's getting harder for institutional investors to ignore cryptocurrencies'*. Retrieved from Business Insider: http://uk.businessinsider.com/goldman-sachs-cryptocurrencies-bitcoin-ethereum-icos-2017-8?international=true&r=UK&IR=T

Wilson, S. (2016b). *Order starting to emerge in the Blockchain chaos*. Retrieved from Constellation Research: https://www.constellationr.com/blog-news/order-starting-emerge-blockchain-chaos

Wilson, S. (2017b). *Julian Assange quoting blockchain hash does not prove he's alive*. Retrieved from Constellation Research: https://www.constellationr.com/blog-news/julian-assange-quoting-blockchain-hash-does-not-prove-hes-alive

Wilson, S. (2017c). *Synchronous ledger technology (aka blockchain): The companies to watch*. Retrieved from Zdnet: http://www.zdnet.com/article/synchronous-ledger-technology-blockchain-companies-to-watch/

Appendices

Appendix A: Biography of interviewed experts

Robert Currie

Robert Currie is the CTO of the Genomics Institute at the University of California, Santa Cruz. His career starts at the beginning of the modern internet age. He has been through six companies coming from different technological backgrounds such as digital audio, the internet itself, geo-spacial navigation. From 1994 to 2000 Mr. Currie was a VP engineering for an early java company with customers like Morgan Stanley, Goldman Sachs, FedEx, and Home Depot.

Jasper Roes

Jasper Roes works for the Kadaster as a senior advisor in the department that is responsible for the product and process management of the national services that the Kadaster is offering. One of Jasper's roles is the role of product owner for the Kadaster Dataplatform. The Kadaster Dataplatform transforms existing data sets to Linked Data, including semantics, and publishes the datasets as Linked Data through a SPARQL endpoint and API's. Next, to that Jasper is involved in the block chain activities of the Kadaster.

Maarten Everts

Maarten Everts is a Research Scientist at TNO & Assistant Professor at the University of Twente. He is an expert in the fields of Information Security, Applied Cryptography, Privacy Enhancing Technologies, Identity Management, Security Engineering, Smartcards, RFID & NFC. He is a specialist in block chain technologies, with a focus on security, smart contract security, cryptography, privacy, and identity management.

Stephen Wilson

Stephen Wilson is VP and Principal Analyst at Constellation Research. His main focus areas are digital identity and privacy. He is an expert in identity management, frameworks & governance, digital identity technologies, privacy, big data; identity & privacy innovation. Mr. Wilson has worked in ICT innovation, research, development and analysis for over 25 years. He is a specialist in cybersecurity and identity management. Mr. Wilson has provided advice on national ID frameworks to the governments of Hong Kong, New Zealand, Australia, Singapore, Macau, Malaysia, and Kazakhstan. He is a block chain critic and argues that non-monetary use cases for block chain do not line up with the original block chain idea.

He advocates careful and sober requirements analysis around what he calls second and third generation DLT. Patents: - *System and method for anonymously indexing electronic record systems* US 8,347,101; AU 2005220988 - *Authenticating electronic financial transactions* US 8,608,065; US 8,286,865; AU 2009238204; NZ 589160

Christopher DeRose

Christopher DeRose is a public speaker, software developer, and journalist. He is the lead organizer of the South Florida Bitcoin group, he is also a lecturer, and has his show on YouTube called “Bitcoin Uncensored.” Recently, he was pronounced as one of the most influential people in block chain according to Coin Desk.

Erich Erstu

Erich Erstu is a software developer and owner of cryptograffiti.info - a service that allows people to encode hidden messages and hashing of documents into Bitcoin’s block chain. Most notably, it can produce proof-of-existence time-stamps and upload JPG images to the block chain. Cryptograffiti.info is a web-based service that can also be used from a smartphone rather conveniently. The web interface is released under MIT license, and its source code is publicly available on GitHub. The backend solution that actively monitors the block chain for new human-readable content is private.

Jaco van de Pol

Jaco van de Pol is a professor of Computer Science at the University of Twente. He is the Chair of Formal Methods and Tools research group, where tools and methods are developed to support the development of software. He is also the Head of Department Computer Science within the faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS). His research interests are in modeling and analysis of safety, dependability and security aspects of software-intensive embedded systems. Application domains include embedded systems, distributed systems, security protocols, and biological systems.

Maqsood Ahmed

Maqsood Ahmed is Technical Fellow at PACCAR INC. Seasoned Unix administrator (AIX, HPUX, Linux). ESX Administrator. Windows Administrator (Windows cluster). Support Weblogic, PLM software, Apache Web Server. PACCAR had few meetings with IBM on block chain implementation and had not yet made a decision where this technology could be most useful.

Appendix B: Interview with Jelle ten Hoeve (Preliminary research)

The Netherlands Cancer Institute (NKI) is a comprehensive cancer center, which means they provide services directly to cancer patients through the hospital Antoni van Leeuwenhoekziekenhuis which specializes in oncology and which shares the same building. Sharing the same building helps the institute with research and the hospital with newly developed treatments. The hospital only accepts cancer patients and approximately 10% of all cancer patients in the Netherlands have a data footprint there. The institute does basic research lab work including translational research and clinical trials. It has extensive biobank materials and archives. Through a national organization supported by philanthropy, it performs the $1000 genome sequence – which costs for a whole genome sequencing an individual or patient roughly $1000 (Wikipedia, 2017d). Currently, genome sequencing is highly centralized by one company called Illumina LLC from the USA. The costs for such a sequencing facility amounts to several tens of million dollars, of which data processing and storage take a large part. It has a yearly capacity of 7000 patients.

Appendix C: Interview with Wayne Vaughan and Chris DeRose (Preliminary research)

Tierion can generate a receipt from the data that goes into the block chain, and the information on the receipt is enough to verify the data. Mr. Vaughan said that there are multiple ways to commit a hash of data to a transaction that is invisible. He calls them "invisible anchors." Pay to Contract Hash is one such method. Another option is to commit data to a Bitcoin transaction in a way that does not have a long-term impact on the chain. For example, including data in OP_RETURN (which is prunable) transaction, and construct a proof that creates a commitment path back to the Merkle root of the block header. That allows proofs to validate even if the OP_ RETURN data is pruned. The Merkle roots are the links that hold the block chain together. If the proofs commit to the links, then they are unlikely to be affected by a future change to the block chain.

He refers to his protocol as "trust anchor" rather than the standard "time-stamping." He sees it as more than just time-stamping mechanism because time-stamping implies that a person is trying to determine when something happened with a high degree of precision. The name of his company "Chainpoint" implies that it serves as a pointer to a transaction on the block chain. The real value of Chainpoint is a trust anchor that cannot be corrupted and is replicated across a global network and on multiple chains. If there is a need for a time-stamping solution, the world is full of them.

Tierion has the ambition to create a standard in the scalability of anchoring data, and the World Wide Web Consortium (W3C) has recognized Chainpoint, the underlying protocol of Tierion, as one of the three block chain technologies to move forward its standardization process (Waterman, 2016). "Tierion turns the block chain into a global platform for verifying any data, file, or business process." (Tierion, Inc., 2017)

Tierion is well respected in the industry and considered one of the honest block chain companies. In a short interview with Chris Derose from the YouTube show "Bitcoin Uncensored," he recommends using Tierion if someone needs a block chain for something. It is easy, efficient, and there are no tokens. Moreover, it is more secure than anything else on the market. Chris Derose is a proponent of the idea that companies should not tokenize their projects. However, it should be noted that as of August 2017 Tierion has tokenized its services.

Appendix D: Interview with Robert Currie

Block chains and the internet

Mr. Currie compares the block chains to the internet and that we can substitute the word “block chain” and change it to “Internet,” and the conversation will still be the same. For example, in 1994 it was unimaginable for people that one day they would be going to not only enter their credit card info into a computer but also that they can spend thousands of Dollars on products purchased on a website. Nobody would have thought they would enter their credit cards and buy products. This narrative can be compared to the narrative of block chains.

Another example that Mr. Currie gives is about the early perception of video streaming over the internet that it was considered impossible at first and even people believed it was not scalable. The way we time our entries in emerging technology is a key, and we always overestimate the short term and drastically underestimate the long-term perspectives. Most people have drastically overestimated the short-term perspective in the block chain. There is some fundamentally sound technology that we can use.

Genomics

Computer scientists solve problems every day, and they look for solutions in their available skill set and their “bags of tricks” or their set of ingenious plans, techniques, or resources. One of the projects that Mr. Currie had to solve was a distributed ordered list and about one year ago he was working on a project called the Cancer Gene Trust (CGT).

The CGT finds people and gets them sequenced, and the trust pays for the sequencing. There is much bureaucracy around doing it, and that is because it does not have up until recently a practical use in clinics. However, we are at a point in time in genomics where it is obvious it is going from research to practice. Mr. Currie believes everybody that is going to a hospital at some time in the next ten years will be sequenced or most babies that are born will have their DNA sequenced before they were born.

Illumina is the dominant company in the sequencing of DNA, but the spectrum of businesses is growing – for example, there is a company in California called Pacific Biosciences, in the UK there is a company called Oxford Nanopore that has created a USB thumb drive DNA reader. The technology in what is called Nanopore sequencing was invented at UCSC. Moreover, it has been used to sequence Ebola in Africa in the fields, so no one has to send the samples back. Nobody wants to receive Ebola in the mail. It is also used at the

International Space Station (ISS) because it enables sequencing in non-laboratory environments even in microgravity.

There is a tremendous opportunity here with genomics because we are living longer mostly due to clean water and eventually if we come up with solutions to every other problem we will drastically increase the quality of life. Most people most likely are going to die of cancer. Heart diseases are the number one cause of death in the world today, and it has come way down. Cancer is number two. 80 million people a year worldwide are diagnosed with cancer, although cancer is not a disease. It is nature; it is evolution gone wrong. It is like driving a car enough miles, and eventually, it falls apart, or the handle for the window eventually falls off. All in all, cancer is genomics. It is a program. What is going on with genomics and computer science is breath-taking. Moreover, its impact on humanity is high. The ability for genomics to both drastically increase the quality of care and drastically reduced the cost is incomparable, it is tough to come up with something that has a more significant impact in the long run. Mr. Currie thinks that the long-term might be five years, could be ten years, and could be 20 years, potentially, which is just a blip. There is plenty of studies now and "precision medicine," which can be classified as a customization of health care, can tailor treatments to people with aspects of early detection. The best thing people could do for cancer is to find it early and the way to find it is in the blood and find circulating tumor cells by sequencing them.

The impact on genomics is potentially huge, and that is one of the reasons Mr. Currie switched to that field. Just like the internet, it has the chance to radically reduce the cost and improve the quality of everything and save and preserve human life. For example, sequencing helps children receive proper treatment when diagnosed with cancer. The institute receives sequenced data from tumors from children who have cancer who have no other option. They run a bunch of math on the data, and ten days later they come up with a list of drugs that might fix those children.

Exhausting data

People exhaust data in clinics. In fact, people exhaust data all day; they leave so-called "digital breadcrumbs" all over the world. Moreover, as Marc Andreessen said in an essay for the WSJ "Software is eating the world." Nowadays, Medicine is data and software, DNA is information and life itself is information. DNA is Mother Nature's 4.5 billion-year-old information economy. DNA is an exchange of transactions, and there is more information stored in DNA than we will ever be able to store on computers worldwide. There are more transactions done on a cellular basis, on organism basis than the entire financial market. So, we could say that “Medicine is going to be eaten by software.” We can take information out of our bodies through an increasing array of techniques. The USB gene reader mentioned earlier can cost $20 to sequence a sample in few years, today it is about $1000. We can assume there is a massive market for extracting information from our bodies for economic and health reasons. This is already happening for example with taking blood pressure.

Famous VC, Vinod Khosla, talked to the head of Harvard and Stanford’s medical school and he said they had it completely wrong. All of the diagnosticians are not in their school. Instead, they were in the math department. All the doctors in their group will just become counselors because the patients will be in control of their entire medical world. The patients will have all the information, and this will be the revolution in health care. Just like in financial services where people used to rely on brokers to do all the work for them, do all the analysis and do the right thing (even though sometimes the brokers were not doing the right thing), it was found out that people can just as well read and understand investments and make the right choice with some guidance. Just like in financial service, we can extrapolate the same narrative into health care. People can be their guardians of their data and make their own decisions. Mr. Currie is also convinced that technology is going to drastically change and or eliminate big pieces of the medical world (for example the radiologist's job will be gone), because of deep learning algorithms that are already superior to humans.

Last year the CGT proposed to build international distributed system to store genomic data. The issue with cancer is that the data sets are always too small for research. They are usually in the order of 10 000 data points. In other sectors like speech, image, text mining when someone applies machine learning to a domain it becomes better than human very quickly, but it needs at least 1 million data points. If the clinic is going to be generating all this data, it is better just to figure out how to exhaust it directly out of the clinic, make it accessible worldwide so all the algorithm designers can access it, build machine learning models on top and deploy those out to the clinic as well. That is the big picture of machine learning from genome data.

Prototype

The CGT built a prototype on Ethereum a year ago where only the submission was on the block chain. The data was stored off-chain. They were using IPFS for the data storage and

Ethereum for the submission (referencing). They are using IPFS because putting someone's whole genome data out there might need 200 GB of space. It would cost a fortune to put 200 GB on Ethereum which currently is in total 220 GB. For example, the CGT can put 200 GB of data on IPFS and then reference it into a hash on the block chain. In IPFS hashes are the links to files. Instead of using names IPFS uses hashes. Anyone running an IPFS node could access the file using that hash. Also, data on IPFS can be made private so that only specific nodes can have access. The idea of IPFS is that a hash cannot be fabricated or created to access specific data. A hash is the digital representation of a file in a minute form.

The CGT's goal was to create distributed platform for sharing data among clinics**.** Using a block chain directly tied to the process created additional problems to deal with. Furthermore, ordered list was not as needed as it is in the financial world where having it is a must. If there is no requirement for order, there are a lot of other ways to generate a distributed list. If a clinic does not care whether someone published a piece of genomic data yesterday or today or who published it first, then there is no need for a block chain. For someone who is considering using a block chain, the qualifying questions come down to whether there is a need for an ordered list. If there is no need to have an ordered list then block chain offers a very complicated way to solve problems.

The CGT findings from their block chain prototype showed few main challenges: 1) the marketing problem (that is maybe gone away in recent months), 2) how to set up miners and how to get people incented to do mining, 3) when the actual management of the list becomes more financially valuable than the real problem the entity is trying to solve in the first place and 4) does the CGT or any entity need an ordered list.

Misconceptions about block chain

A misunderstanding in health care is that people think that a block chain or software will solve all of their disagreements on how to describe something, how to explain something. Software is not magic, and it does not solve the interpersonal behavioral problems people have. For example, someone can call something blue, and someone else decides to call it red, and both can enter that misinformation on the internet on a block chain. People can anchor lies on the block chain. This problem of disagreements is tidily connected to politics, sociology and the human nature. Some people expect block chains to fix health records. Doctors have been around for thousands of years, and their notes are usually a disaster, a mess. They are not famous for taking notes carefully. So, even if their notes are electronic, someone can look at the electronic record and can see that one doctor has called something blue and other has called it red and it is in a block chain. Even if we discern provenance and order, there is still the fundamental problem of someone calling something blue and someone else calling it red. Truth stays subjective to the person entering the data.

Price is the most efficient uniform worldwide recognized marketing tool. If someone can give one unified information about a product or service that would be the price. Price is a powerful way to communicate information about a product or a service. It is a straightforward tool; it is just a number – value. The block chain has been very successful in trying to capture a single value, quantity, and it is a lot more complicated than capturing value in traditional markets. If someone is trying to do something with value, then the system works very well.

However, if someone is trying to exchange something significantly more complex, then they might have a problem. For example, Ethereum added Turing complete state machine that allows people to write contracts. Contracts are an attempt to codify human interaction, and it is not only just about the value. There are always conditions in contracts: what happens if this happens, what happens if that happens. Also, contracts are messy, and hard because of human interactions. DNA is maybe the oldest piece of digital information but humans are still analog creatures, and block chain is not going to immediately magically simplify human interaction unless human interaction is simplified down to price**.**

Benefits from a business perspective

In the financial world, the order list is essential in financial transactions. For computer scientists at an investment trading firm, block chain is immediately evident as the replacement for the stock exchange. However, for the CGT the order list is not of great importance, so the trust chose to stop using the block chain project last year. In the financial market there are many reasons why block chain is beneficial, and maybe even it will cause the downfall of legacy exchanges and maybe the end of the Federal Reserve. In the end, probably there will be a giant market that it is going to be built on block chain technology regardless of what anybody else does. The internet would not have happened to build Instagram if it had not have built Amazon first. The fact that it was already there made Instagram easy to build, but nobody would have built the web to do Instagram. The financial markets would probably help bring down the scale and the cost in understanding and accepting Bitcoin.

The concept of the CGT is, for example, anyone to be able to walk into a hospital in the Netherlands, and the hospital to be able to diagnose whether he or she has a tumor. They sequence it and do a biopsy. Consequently, the idea is to figure out how to exhaust some of that data out of the clinic directly and share it with the world right away instead of paying for research studies. Humans walk in a hospital, and they will be sequenced (their tumor, their DNA).

Opportunities with block chains

Block chain solves a problem for which computer scientists have struggled to solve for decades. The issue of how can we maintain an ordered list with no central point of control, which is a tough problem. In computer science, this problem was always solved with having one central ordered list. Computer scientists will always build something that will maintain an agreed upon ordered list with a central server. No central point means that there is no single point somewhere that is responsible for being the arbitrator of conflicts or the ultimate source of the list. Every solution computer scientists found to this problem they always came up with one central point.

The issue with having a central point breaks down into two different problems; that it can be a central point of failure for a system and from a social standpoint it means that everybody has to agree to trust that one entity - the master ledger (the central point). We can sum it up as “in God we trust, all others must bring math.” Block chain solves those two issues with math. Mr. Currie has confidence in the solution Nakamoto came up with regarding the math in allowing for an eventually consistent ordered list. Eventual consistency is a model in computer science in which the system guarantees if no new updates are made, “eventually all accesses will return the last updated value.”

Opportunities for cryptography in health care

Genomic information imagery is extensive, and it has many issues around privacy. The Germans, for example, are anxious about genomics, partly due to the history of Mengele and World War 2, and partly they believe that the NSA and the spies in the US can use genomics information to spy on the Germans. Canada has laws where clinics are not allowed to move the actual sequenced data across provincial borders. Moreover, soon in 10 years, it will be all entirely possible for people to be able, for example, to pull a hair off other people’s shoulders and put the sample on a USB gene reader that is attached to their iPhone. Then the application will give the statistical odds of the person they just met to develop Alzheimer's, is an alcoholic, the chances that any offspring that person might have any of 1000 diseases. People will also be able to know the statistics for a lifespan or what the chances they are going to live extra ten years. This creates complex issues especially for creating life insurance markets when people can predict who is going to live longer and who is going to live shorter.

The CGT's proposal for the privacy problem is to divide medical information into two different categories: de-identified data which is useful for researchers to build better machine learning algorithms but by itself that data cannot be used to identify someone, and identified data. For example, if someone came up with a database about the shoe size of each participant on the NKI conference, then it probably would not violate everyone's privacy because that database contains just the shoe size.

In cancer every single cell in a tumor is different. It has been mutated from the DNA by a variety of reasons. The CGT proposes to allow patients to be able to publish and share the errors in their tumor on the internet. Data cannot be traced back to the patients because the CGT cannot figure out generically how to trace a tumor back to a person. The information will be signed with a random identity. For example, the NKI holds and protects all the personal information of patients, name, DNA, and everything else because patients trust the NKI. In this case, the NKI is called a steward. Then the NKI sends the de-identified data to a machine learning algorithm. The algorithm should have access to the actual DNA to train and then send back only what is called the "weights," "the model." The model is a smaller number of values. For example, if the NKI has a million genomes and each one of those genomes is 3 billion base pairs. The weights of the algorithm that are sent back have only 60,000 values because it is possible to encode a million pieces of DNA in only 60,000 values. So, if the NKI looked at the wire and saw that only a packet of 60,000 values came back to the CGT, they could be fairly confident the CGT was not ripping them off. They were not just exhausting all of their data out. The CGT wants to learn from the data; they do not want the data

The main problem is that a training algorithm requires 100,000 USD in computer time to run on today's systems. For example, the NKI has a million genomes stored on their server that they protect. If the UCSC would like to train their neural network on the NKI's 1 million genomes, the UCSC will send the code through a "docker," which is for everyone to use. Then the NKI will run the code to give back the 60,000 values, but it will require 30 000 GPUs per 1 hour. That is much money.

Risks in block chain for health care

Late last year, the CGT started talking with clinics what they want to do. Coincidentally, a hospital somewhere in the USA was hacked around the same time with all data kept hostage for ransom for payment in bitcoin. So, that made it hard to talk about block chain and Bitcoin because it was always understood as something untamed and used for crime. The conversations were bringing topics about hacking and criminal use. Anecdotally, we can make the analogy with medical care that uses US dollars and the drug cartels which also take dollars for drugs. However, that does not mean medical care should stop taking money. Consequently, it became apparent that from marketing standpoint block chain and Bitcoin were a bad thing. Mr. Currie together with the CGT decided to take out the block chain aspect and just use IPFS. Nowadays, the unease opinion about block chain has calmed down, and people do not associate it solely with hackers.

There are some general issues with block chain that on the financial market do not pose a problem but are hard problems for health care. In a block chain, there has to be one chain; there should be a chain that everyone agrees upon from its beginning marked by the creation of the Genesis block (the first block). If, hypothetically, the CGT created own block chain for their prototype with own Genesis block, then, anybody else who wants to contribute to that chain can add to it via the block chain. However, the problem in the medical world is that the maintenance of this list, which is directly proportional to the number of people mining the list. The way that agreed upon list works is through techniques like PoW which requires having many miners. In the financial market, it is all about money, so there are huge incentives to mine. If we are trying to maintain a list of genomics in the medical world, there would be no incentive to mine.

In health records, if there is a created list of medicine that someone takes, there are very few scenarios when a doctor would require to know for sure the exact order of that list. For example, the scenarios when 1) someone needs to get into the drug treatment, or 2) when someone who is known to be a drug abuser and a doctor wants to verify somehow the order of prescriptions they received. These examples would require for physicians and scientists to need ordering in the health market. So far, Mr. Currie says he has not seen where it is an absolute must to have ordered list in health. Moreover, if there is no need for ordering, mining is a complex and messy business. If there is no requirement for the order, then there is no need for mining.

Public-key cryptography and health care

Technologies for public-key cryptography are well understood, there is plenty of libraries, and it is a highly standardized area. Today, the CGT which is still a prototype will probably have its first submission in about a month or two. The mechanics of the setup will allow, for example, the NKI who created some new data to publish them onto the IPFS world which is distributed; then they will sign that data by using their public, private key pair. The NKI can create their list of data, and that would not affect other parties because all other parties only care about whether all these data come from the NKI. This method does not allow to be sure when the NKI published these data; there is no time-stamp on the data. Of course, the NKI can put a time-stamp in there, and the trust is all based on knowing who the NKI is and knowing what the public key is, so others will know specific data must have come from the NKI. Again, this shows that if there is no need for an ordered list, then this becomes a drastically more straightforward problem to solve.

All in all, the conclusions the CGT made from their experience with their prototype were: 1) mining is expensive and complicated if they want to do it on their own and 2) there is no need for order. Therefore, they can just do a distributed system.

In IPFS, every hospital can point its peer to another hospital and eventually could connect to the whole network. New users can join by finding a peer from the network and send a request for joining. In the network that the CGT built, new users can speak to the NKI or the UCSC and convince them to point to them to join their network. If there are bad actors in the network, no one will point to them.

IPFS has a feature in it called IPNS (InterPlanetary Naming System) which is much more straightforward and what it does is public-key cryptography. Public-key cryptography has been around for about 20 or 30 years, and that system gives provenance, which is essential for the medical world. It is central to have confidence in the accuracy and the quality of newly mined genomic data. Apart from only being able to run an algorithm to determine the quality of data clinics also need to know who provided them exactly. For example, the NKI and UCSC are trustworthy, and they have sound quality operations, so an entity would only like to know whether specific data came from them. An IPFS server generates a public-private key pair automatically. Anyone can publish a hash of all their data on an IPFS server, and they can sign that hash with their public, private key pair. If someone knows the public key of the NKI for example, which can be publicized, he or she can ask the NKI if a specific piece of data comes from them. Anyone can verify the origin of data by verifying that the digital signature matches the public key and the only person who can generate that signature is the holder of the private key. That is all that is needed; no need for an ordered list, nor miners. All that is required is to know the provenance**,** to be confident that a specific entity produced given data. All that is needed are public and private keys and nothing else.

In block chains, there should always be just one list (one chain) originating from the Genesis block. If users are not concerned with the order and only need to quickly find one another, they can use IPFS which solves that is by building a network of peers. There is no central authority worrying about users being able to exchange information in IPFS. Doctors and scientists in clinics most likely do not need to make sure that there would be one list of all of the hospitals in the world.

Block chain as an economic opportunity in health care

In 20 years from now, health care worldwide can be entirely revolutionized and switched to a model where every day there is tons of information that is exhausted from humans and data are continually changing because Mother Nature is changing. Nowadays, scientists realize that no one is going ever to figure out how to solve everything. Things can never be static because Mother Nature keeps changing. There is always going to be something that comes up. In fact, for example, humans are now impacting the world, with global warming by impacting it with chemicals. Humans are changing Mother Nature every single day. Therefore, they will have to build a worldwide system that continually evolves and computes new ways. They need to have the information that is being exhausted from organisms worldwide, flow it up into a digital form, and make all machine learning algorithms that are running around the world learn from the data and figure out what to do, and feed that data back into the economy. This economy of health information and computation feeds itself by improving the quality of life of every man, woman, and child on Earth.

Block chain is successful if it enables a whole bunch of individuals, organizations or entities to work together where they would not have worked together otherwise. Furthermore, block chains scalability is not worrying. Old technologies will still be around and still exist, so there will be alternatives if ever block chain fails for some reason. Scalability issues with block chains are not worrying. For example, the internet allows video calls for free, and that was impossible to even imagine in the early days of the internet when a video call could cost around several thousand dollars across the Atlantic.

Infrastructure

There is a two-day conference in Palo Alto about health information and computation, about this concept of sending computation request to someone for examining their data and they send back the results. Mark Zuckerberg and his wife formed a foundation called Chan Zuckerberg Initiative (a massive project that they are funding) with the goal of curing all human disease in the next 80 years or during the lifetime of their child. A worldwide group of computer scientists is meeting in Palo Alto in a month to hash out little details. The conference is literally about agreeing on how to send computation and how to send results to a standardized gateway. The goal is to map every single cell of the human body worldwide as a first step in the cure of all human disease.

A side effect of that project is a whole bunch of institutions worldwide is going to agree on how to send and receive computation over medical data. Not using block chain, Zuckerberg will pay for the computer time because all parties agree that they are going to use their computing resources. At the end of the project, in 4 or 5 years, the institutions involved in the project will have a very robust way of sending code round and had it run and send data back.

During the time of the project, the business people in hospitals have to figure out how to build this worldwide economy between all the businesses in clinics. Talking only to the computer scientists and the clinicians is not enough to decide who is going to care to run this 100 000 hours or computational time. The CEOs of the hospitals have to get involved because they are the ones who worry about the investments and money. Looking at the database system that runs a hospital the most relevant table is called “beds” and the management of beds is one of the responsibilities of a CEO in a hospital. That should change in the future because medicine is going to be an information business and that is going to be a revolution for the business people in hospitals.

Appendix E: Interview with Jasper Roes

Use case in open data and permits

Kadaster has a block chain project but not so much with notary because it is proven to be more difficult. They have a project with open data and how can people use the block chain to ensure that for example when using specific open data to ask for a permit that it is the correct data and later prove which data a consumer has used.

Eventually, the targeted audience for the product will be the end users, mass consumers, and also architects and people who have to ask for permissions concerning building a house or making an extension to the house.

Benefits of using block chain

The users should not be worried if he or she is using a block chain or something else. However, they should see more advantages, for example, cheaper service and more transparency. The benefits for consumers, should not be affected negatively by using a block chain.

Now, block chain is knowledge push, but in some years the knowledge push will be over. So, everyone involved will just need to find the most suitable solution which can provide all the things that the user wants. In the end, users would not prefer a product just because it is a block chain solution, but because of the benefits, it provides.

Users will most probably not be able to recognize they are using a block chain for their needs. Just like most users now do not realize most of the processes involving technologies and how they work. The technology just needs to work and be beneficial (cheaper, and technologically better).

Opportunities in using permissioned block chain

In addition to the proof of concept, Kadaster also had strategic sessions with advisors to discuss whether permissionless or permissioned block chain was better to use. The conclusion for their specific use case was that permissions in a private block chain seem more feasible and logical. Private permissioned block chain removes volatility risks because there is no token as in public permissionless block chains. The thing with permissionless block chain is that one cannot guarantee how expensive it would be to do validation.

Furthermore, Kadaster considered not to have permissionless block chain because if several thousand nodes are validating work, it can be less efficient and especially cost intensive in the end. However, outsourcing the validation to a public network can save some work for Kadaster because they will not need to do all the processes themselves anymore. So, it might become cheaper for a while, but it is unsure whether it will stay that way because public block chains are volatile.1) Immutability of data which people can use for all kinds of proofs. Hopefully, in the end, it would be impossible to change the ownership of an individual or a piece of land without having some proofs that someone changed it. If someone changes the ownership, it will be noticed and asked that someone changed the data and whether the person had actual permission to do that. 2) Trust and 3) transparency are also important traits of a block chain for open data use case.

Trust becomes very necessary if only Kadaster is validating. To further improve the trust Kadaster will have to make their system open and publicly available. Then they will need other parties to validate Kadaster's work because otherwise, Kadaster will still be the only one validating. The trust issue is of high importance, and they want to make the system as transparent as possible with the high degree of provenance. There is no issue in the trust in the current system of Kadaster, and at this moment there is no case to require it, but they want to continue experimenting with block chain and see how they can further improve the trust.

Even with using a block chain, there is still a need for a TTP to ensure that processes are correct that no one takes the data and move them somewhere else. There will always be a need for someone responsible for that. The utopian idea that because of the block chain people can remove all third parties like Kadaster sounds nice but not realistic because, for example, someone has to be in the actual area of the property to create the proof. Moreover, in the end, also a party is needed at least to operate the block chain to ensure that not just everyone can change the data there.

With the block chain, people can even prove that there was no more data in the database. In some processes, most of the times there are cases in court that something additional pops up and judges can say that it was there, but the person never saw it. With block chain that could become impossible because of the data transparency.

Permissioned block chain

For the moment, Kadaster needs to have permissioned block chain because they want to control who is validating and who can write to it and it seems logical for such kind of business solutions. Eventually, it would be good also to include notaries to have permissions to be able to validate and write next to Kadaster.

First trial

Kadaster made their first trial with block chain and showed it on the market to some companies, and it was not a proof of concept yet. They wanted to see how far they can go and how it would work in the end. Kadaster did not care about the block chain they use; they only care about a proof of their concept that it can do what they anticipate and plan. The hired company did the integration part and the front end. It implemented MultiChain as block chain engine which is a free software for building private block chains. They had strategic sessions with consultancies to see what can block chains do and what is not possible. A similar solution could also be done differently by other software.

Kadaster uses MultiChain for their implementation, but when they want to start using smart contracts, they will have to move out of MultiChain. The only reason chose that application is because the company they hired had a great experience with it. They did not care about which block chain solution to use.

Validators in Kadaster's private block chain

Kadaster intends to look for a minimum viable ecosystem where some parties will be able to validate but also will have only read-only copies to the database. So, in the case, the main database is down (even though there is no main database in block chain) at least Kadaster would be able to do validations. Moreover, depending on how many parties can write on the block chain it will be able to continue the process of operation.

In Kadaster's PoC, a validator could be any company that also offers consumers efficient way to handle permits. They can use Kadaster's block chain implementation or a combination of block chains (all the block chains they have with multiple parties) to validate proofs. They can validate the correct data and also prove it that is from Kadaster but Kadaster are not interested in being part of the actual permit process because it is not their business. At the moment Kadaster created their front end just to show the PoC and to keep it simple, but in the future, they hope that other companies (third parties) will set up their front ends. Kadaster only offers the info and the block chain and the way to validate it.

There is no idea yet how much it would cost for a person to validate their contract on the block chain because most of the concentration of Kadaster at the moment is to open data. They are looking at land registry, but they are not so far with it.

In future, if Kadaster does not do all the validations themselves, it might be that Kadaster needs less computing power because they will have only one node for example and all other companies are sharing nodes with them together to define what is true and what is not.

Future of block chain beyond payments

Block chain is becoming relevant in notary services. The critical question is how different notaries are going to be using it. Whether current block chain solutions have a future is debatable. Businesses just need to learn what they can do and how certain parts of the current block chain solutions they can implement.

Measure block chain development

It is hard to measure transparency and trust in a block chain because they are subjective factors. However, lower transaction costs and people using it are reliable benchmarks. It becomes cheaper because if people use a block chain, they do not need third parties like Kadaster anymore for specific processes (they become automated).

Block chain proofs in court

Whether time-stamped documents or proof of existence hashes on the block chain have any weight in court is still unclear. Kadaster is developing new PoC in which they also want to dive deep into the methods how it would work in a court to prove in front of a judge. They do not have a clue yet at some time if for example in the future someone uses the block chain for his or her documents and end up in court what would be the judge’s reaction. Will he or she realize it is true or will he or she not know how a block chain work.

Appendix F: Interview with Maarten Everts

Costs in permissioned block chains

There is no real research yet calculating the costs for running a private block chain. With public block chains data is more available and can be compared and mathematically calculated certain expenses for mining or validating. Hardware costs, energy consumptions are open information. However, for private block chains, this information is still not very clear. What is the cost for using a private block chain and how to price users is unclear? Who pays the programmers, government license, what business models to create, how much is the electricity costs. How can all this be factored in the transaction fees is still a big question. Because block chains are global, there will be differences in jurisdictions and energy costs.

Private block chains are more attractive for business use cases, and that is where the money is. However, at the beginning of the internet, it was also considered to have private internets – Intranets, which eventually became connected to the main public internet. Here, we could have the same situation where private block chains are used for business because of their speed and high performance and higher predictability and be connected to a big public block chain like bitcoin to anchor its data sometimes. A good example is side chains solutions. There could sometimes be one block chain that all block chains will be connected to which is a possibility.

Benefits rely on people’s collaboration

In computer science services are usually done by a central authority, a central computer. Block chains are useful because they provide security by having no central point of failure. There is no central server or a computer, and there is no master ledger. The system provides all computers with the same data at the same time without the need of a centralized source.

Opportunities in suppressed countries

Block chains are an exciting mix of game theory and economy. They are highly more scalable than previous distributed systems; most BFT consensus protocols can only scale to up a certain amount of nodes. Traditional systems are also limited by the company that controls the nodes. With block chains, scalability is greater, there can be an infinite number of nodes, and any business can participate; anyone can ask for permission to join the network or in the case of permissionless block chain there is no need to ask.

Risks to privacy in public block chains

Also, there is no room for mistakes. Mistakes are severely punished because transactions are non-refundable. There is no one to call and no one to sue. Everyone depends on a machine to make the arbitrage decisions. Another risk is when the marginal return for someone to exploit and manipulate the block chain becomes higher than the marginal cost of attacking it. Then, people with enough money could reorganize the block chain by a 51% attack if, for example, they know there is something on the block chain that is more valuable than the cost it will take them to attack the chain. For example, acquiring the ownership registry of an expensive land or emptying the account of a wealthy investor.

In public block chains, tx fees are priced based on several publically known factors. They reflect the model and are publically available for analysis. However, sometimes fees can become very high. If the price of the token is increasing the fiat equivalent of the fees is also increasing. Bitcoin’s price has increased ten times for the past two years, which means that its transactions costs have increased dramatically. Ethereum was a block chain with low transaction fees until it went ten times in 2017. Public block chains are volatile because they have a token to incentivize the miners which can create complications for creating business models. Currency risk, volatility, and tx uncertainty are all very high risks for business users.

Block chains are machines and operate as programmed. Smart contracts are coded laws that cannot be changed. There are no ‘buts’ in smart contracts. They cannot be modified. That makes it hard to rely entirely on a machine to be in charge of legal disputes in the form of smart contracts. There should always be a TTP of some kind.

There is still need for a TTP to link the gap between the physical world and the digital world. Block chains are means but cannot be trusted with the creation of proofs. Someone trusted has to enter the proofs. The inputs and outputs, the oracles are essential figures and are needed in connecting block chains with the real-world.

For block chains to have any merit in law, enough people must say it is an authority. It depends on how much people trust the technology to make it viable. People need to accept it to have any meaning in court for proof matters.

Appendix G: Interview with Stephen Wilson

Opportunities for private block chains

Private block chains have more chance in business than public ones. Decentralization was never a necessity for security. It was made for political reasons because the creators of the first block chain were anti-authoritarian. Security does not require from a ledger to run on thousands of nodes.

When the security model shifts from decentralization to centralization, a new set of rules becomes necessary. To maintain the immutability of the ledger when there are no thousands of peer-to-peer nodes, requires “hardware-protected keys, high-grade hosting, high availability, and particular attention to insider threats” In other words, the focus is on the security of the nodes. In public block chains, the nodes are necessary to cope with rogue miners, and compromised nodes are dealt with by the swarm.

Risks from implementation in health care

Mr. Wilson observed from his attendance on the workshop on “The Use of Blockchain in Healthcare and Research,” organized by the Department of Health & Human Services Office of the National Coordinator (ONC) 2016 that no one was able to explain the compatibility of all records with a block chain. Block chain’s primary purpose is to provide unchangeable distributed ordered list, so everything that is on the chain needs to follow one sequence to prevent double spend without an intermediately. Block chains are not interoperable. The complexity in health care is intrinsic and cannot be changed merely with, for example, a new storage technology.

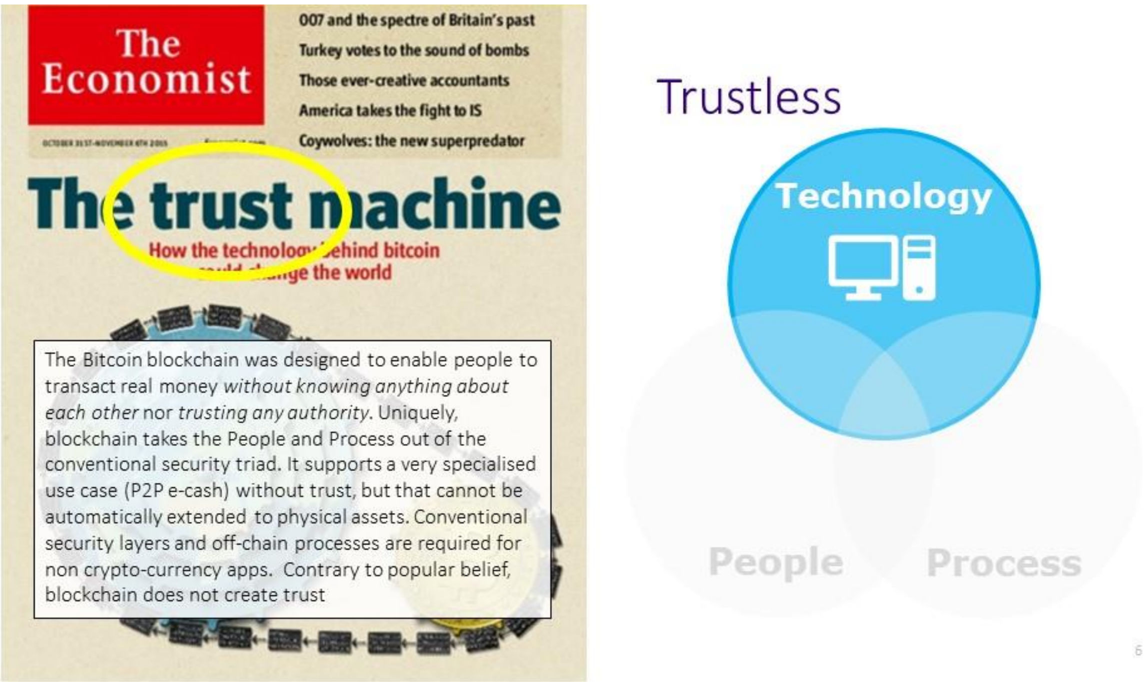
Furthermore, recognizing certain parties, knowing who is who (provenance) in health care important. In the case of Bitcoin, for example, the idea is the allow people exchange value without needing to know who they are, which is not what health care needs.

Moreover, health care requires administrative structures which are in contradiction with the purpose of a block chain which tries to avoid any administrative control. Mr. Wilson reminds us Nakamoto’s statement in the Bitcoin white paper which claims that if a block chain deployment still has to involve third parties, then the benefits of the algorithm are lost.

Mr. Wilson thinks that uncertainty and risk of block chain and ledger technologies outweigh the benefits of using the technology for non-monetary use cases and that is why their relevance to HIEs, for example, is still unclear.

Mr. Wilson concludes that it is unlikely that any single technology can be transformative. So, the expectations for significant health care systems like HIEs to use some ledger tech are tempered, for good.

The following is from a presentation to the IBM Interconnect 2017 conference in Las Vegas in March by Mr. Wilson.


The Economist
007 and the spectre of Britain's past
Turkey votes to the sound of bombs
Those ever-creative accountants
America takes the fight to IS
Coywolves: the new superpredator
The trust machine
How the technology behind bitcoin could change the world
Trustless
Technology
People
Process
6

The Bitcoin blockchain was designed to enable people to transact real money *without knowing anything about each other* nor *trusting any authority*. Uniquely, blockchain takes the People and Process out of the conventional security triad. It supports a very specialised use case (P2P e-cash) without trust, but that cannot be automatically extended to physical assets. Conventional security layers and off-chain processes are required for non crypto-currency apps. Contrary to popular belief, blockchain does not create trust

Trust, security, and decentralization

Mr. Wilson shares that during his first wave of interest in block chain in 2015-2016 (culminating in the US Health & Human Services ONC Blockchain Workshop 2016) he believes he was misguided by an intuition that block chain produced “trust,” “security” and “decentralization” which are desirable properties in e-health. Moreover, he believes he was not well-thought-out because a block chain works without trust. When robust off-chain trust mechanisms are needed (as in health care), then, in fact, the public block chains are rather pointless. Block chain implementation should be viewed case by case based on each of the objectives of the organizations.

Trust is still created off-chain. Off-chain processes are often more critical to the overall outcome and cannot be controlled by the ledger algorithm. When translating (tokenizing) physical assets (for example, land or precious stones) onto the block chain, one must trust the third party entering the data onto the block chain. There is maybe no point of having thousands of computers running around the world to reach a consensus about something on the ledger when the quality of the data rests on facts that need to be established beforehand, often by single individuals like land surveyors or diamond miners.

Block chain’s “security” qualities are peculiar to cryptocurrency, and do not extend easily to other use cases; in particular, adding confidentiality to block chain requires a level of key management that is incompatible with the public block chain’s premise of trustlessness and zero administration.

Moreover, the idea of decentralization was *axiomatic* in the block chain architecture, rather than a general result of the architecture. Block chain does not disintermediate transactions in general and does not necessarily change the way health information, for example, is stored or siloed. Block chain is not a “trust machine” or general purpose data security solution.

Appendix H: Interview with Christopher DeRose

Regulatory arbitrage and censorship resistance

Mr. DeRose states that there is no future for block chains in HIEs and legal record keeping. He speculates that the word “block chain” will likely be redefined to mean “journaling” which is a feature already present in all incumbent database systems. He continues by stating that the only use cases that he sees being formed are: regulatory arbitrage (e.g., if someone needs to send $1,000 to North Korea, and the law does not allow to do that with ACH, then he or she can comply with the law by using block chain (Bitcoin, Monero, Ethereum or another cryptocurrency)) and censorship-resistant value transfer. That remittance to North Korea is achieved because block chains are censorship resistant.

Block chain misconceptions

Mr. DeRose comments that there is a misunderstanding about the permissionless censorship-resistant decentralized value transfer characteristics of the block chain. These features have worked to a degree wherein the Marginal Return (MR) of maintaining consensus has exceeded the Marginal Cost (MC) of 51% attacking in the Bitcoin incentive structure, thus far. There are many scenarios where this would not be true for Bitcoin in the future:

- Drugs are legalized
- The SEC regulates ICOs
- An options market develops whereby the MR of 51% attacking justifies the MC of breaking it.

The block chain technology outside of the cryptocurrency space is at best a reduction to error control algorithms, meaning, the checksum breaks and someone knows data has been corrupted (but don't have the actual data). At best, block chain technology outside of value transmission can be described as an error control function. Meaning, that it advertises (and, does not deliver) that it will reduce the number of errors that (supposedly) happen when transmitting data between people. The block chain proponents would have others believe that the reason data records are mismatched is that databases do not reconcile these documents, and block chain will. The truth is much nuanced, and these issues arise through a disagreement on terms, and government compliance requirements. So, if someone sends an email using a block chain, block chain proponents would have people believe that this email is guaranteed not to be manipulated. Email works just fine - and when it does not, it is because people have strange requirements that email could not handle.

Additionally, thus far, the usefulness of the block chain for transfer of value has not been true to any significant degree of scale for any other block chain except for Bitcoin. Most notably in Ethereum, the censorship of the DAO was an exceptional case where social pressures broke the moniker.

Additionally, any centralized block chain (or even a coalition) could be re-written by the key holder, who are theoretically the ones whom would be censoring the data.

Risks from volatility, user experience, and transparency

The risks and inefficiencies are outweighing the benefits of using block chain for non-monetary use cases like in health care and notary. Block chain in health care is always being advocated by people who specialize in neither science.

Not all data is safe to be on the block chain. Value data is relatively safe. Though even then, someone has to have an excellent reason to store the value there outside of speculation reasons. If someone is a drug dealer or debtor who does not want their value confiscated might be interested in storing his or her value on the block chain.

The question about putting things from the physical world remains uncertain because of the amount of trust that would be required for people who enter data in the block chain. That is not different in any way than current models. It would be no different for this problem if block chain were implemented.

Misleading reasons for implementing block chain

Organizations are interested in block chain technology because of inbound links found elsewhere to be applied in a new field. Also, Perceived Social Status for progressive and creative solutions to existing problems is what he thinks drives organizations to be interested in the technology. Inbound links are what propel content to the top of search engines. An article with ten people linking to it will do better than an article with only one person linking to it. If the word “block chain” is included in an article piece, it is a buzzword; then it would get more links.

Impediments in implementation

The biggest cost for implementing block chain initiative is the development. Additionally, if Bitcoin is the rubric for success, which means millions of dollars spent a day in electricity for

Marginal Returns of $0 if there is people see no value. He continues explaining that he does not believe any of these systems will come to fruition. If they do, it is because a vendor slapped a block chain sticker on a product that has nothing to do with block chain.

Some other impediments for implementing block chain are that 1) businesses do not upgrade legacy systems for decades for administrative reasons - MR does not exceed the MC on upgrades. 2) There is a lack of specialized labor in the procurement process. For example, a purchasing manager does not have the technical knowledge required to evaluate the (often fraudulent) claims of salespeople advertising block chain. Moreover, when an educated technical person, like programmer or systems administrator, sees the block chain platform, with veto power, he or she can get the initiative. Because block chain does not solve the problems that it is being advertised to solve. In most cases, it makes the problems worse. Much like they did “Watson” at MD Anderson. Mr. DeRose believes there might be even some sort of a principal-agent issue for the procurement process regarding block chain. 3) There is a lack of an actionable result. For example, in the medical records industry censorship simply does not exist, and when it does, the reasons are regulatory, and not technical. Regulatory compliance is a requirement, and as such, mutable block chains are appropriate. 4) In notary, better systems exist. Guardtime uses newspapers to notarize, and it is more mature and considerably cheaper than using a block chain. Institutions can trust Guardtime because no conspiracy would make Guardtime censor a checksum.

Mr. DeRose also points out in his concluding remark that object-oriented programming in the 90's was a similar fad that had a similar buzz, and a near total bust that was not successful until maybe ten years later, by a new generation that used it in ways incidental to the initial push. In the case of the block chain, he thinks there will be even less success.

Appendix I: Interview with Erich Erstu

Calculating hash of a document on the block chain

Calculating the hash of the contract and storing that hash on the block chain are the hardest parts in the process. In the case of cryptograffiti.info, the hash is also converted to a valid Bitcoin address. This requires prior knowledge of hash functions in general and also how a Bitcoin address is created.

The newly created bitcoin address based on that hash and that hash is different from the transaction hash. A user hashes their document or message and then sends BTC to the newly created address that is based on that hash.

Bitcoin addresses are based on RIPEMD-160 hashes. So any such hash is also actually a valid Bitcoin address. So once someone has calculated the RIPEMD-160 hash of his or her document he or she would have to convert it into Bitcoin address format and send some coins to that address.

Moreover, once someone sends the BTC to that address, he or she can get it back because they have the private key when created that BTC address. Once someone sends the BTC to that address, he or she generated from the file hash he or she are not going to get it back, ever. Those BTC will be lost forever because no one has a private key that resolves into the hash of the file. That is why someone would prefer to send 0 bitcoins to that address, but unfortunately, currently, zero payments are not relayed because most bitcoin nodes think it is spam. Actually, in Bitcoin network spam does not exist because all TXs must have a fee. Dust threshold is currently 0.00000546 bitcoins in most nodes, but this is obsolete, and Mr. Erstu hopes it will be removed in the future. If we were able to send zero payments, then it opens up an opportunity to optimize the UTXO set because 0 value outputs cannot be spent, and thus they do not need to be kept in the UTXO set. Cryptograffiti.info is often criticized because it stores data on the UTXO set, but it only does it because zero payments are not possible. So it is not the fault of cryptograffiti.info that it consumes space in the public UTXO set.

The file hashes themselves have no owner, and thus the BTC sent to the file hashes cannot be redeemed by anyone. There are no private keys to be maintained.

Costs and convenience of storing data on the block chain

If a person knows what time-stamping is, then they can most likely do it on their own because there is no standard for time-stamping that needs to be followed for the time-stamps to be valid. People can store their time-stamps on the block chain in various ways. However, an average user would find it much more convenient to use a service such as cryptograffiti.info than do the time-stamping manually.

The cost to put text on the Bitcoin is not much. Cryptograffiti takes roughly 10% of the fees that are paid to the miners. Since the average transaction fee per byte is fluctuating and the price of bitcoin is also volatile, it is impossible to state a fixed price. At the moment of writing the smallest message costs ~0.0025 bitcoins which in turn is about 5 euros.

For verification, the Cryptograffiti system is not needed at all. Anyone with access to the Bitcoin's block chain can verify a time-stamp. Time-stamping can also be done manually and even if the service is offline people can still use it in offline-mode if they have a cached version of Cryptograffiti.

Opportunities from the block chain bubble

Users are not interested in block chain. Entrepreneurs are interested in the technology because it is in a bubble. Entrepreneurs these days think that they can solve any problem just by throwing a block chain at it. End-users do not care if it is a block chain, a directed acyclic graph (DAG) or something completely centralized working behind the scenes as long as they get reliable service for an affordable price.

Nevertheless, Mr. Erstu thinks that block chain time-stamping could weight in solving legal issues in the court of law.

Appendix J: Interview with Jaco van de Pol

Benefits and reasons to use a block chain

Dr. van de Pol mentions that the primary specialty of the block chain is the absence of a TTP. He explains that block chains create BFT model that involves heavy use of cryptography, and heavy computation (needed to keep the cryptosystem running). Participants have some incentive to participate in the required computations (i.e., bit mining yields some bitcoin credits, but it also is needed to check the integrity of claimed transactions).

General risks

Technology is not yet completely stable. There are many competing alternatives, and it is not clear which one will stay. It is also not clear if one of them will emerge as a standard. Not clear where the actual service runs, or who is accountable for running the underlying service (that might be not an issue in Bitcoin, but some smaller block chains are probably under control of a few people).

Unclear Opportunities

From a scientist point of view, Dr. van de Pol finds the distributed aspect exciting and he is interested in building tools for that can verify smart contracts, since these could empower (non-IT) domain experts to "program" executable contracts. However, if someone makes programming errors, he or she can create much damage (as the example with the DAO smart contract). A challenge is to create a tool that can verify the code written by non-computer scientists automatically.

Appendix K

Interview questions (legal record keeping)

General opinion

1. What is a block chain for you? How do you understand the technology?
2. Which attributes of block chain do you consider most valuable?

Factors influencing organizations to believe in block chain

3. Do you have a block chain project?
4. Who is using your block chain service?
5. What current problems could block chain solve?
6. What (not block chain based) alternatives can solve similar problems?
7. What efficiency do you see in using a block chain where its primary purpose is the transfer of bearer assets?
8. What benefits do you see in using a block chain?

A bearer asset becomes useless if you need to track it into a central database by a central authority and if it deals with real-world assets.

9. Do you know of a working block chain project in your context? Are you convinced it will work?
10. What happens if a user loses his or her private key?
11. What are the costs to implement?
12. Can block chain time-stamping have any weight in solving legal issues in court?

Conceptual questions

13. What are typical barriers and difficulties in implementing block chain time-stamping for contracts and titles?
14. What do you think are the biggest risks in using block chain?

Overview and speculation

15. How would you measure the success of a block chain project in your context?
16. Do block chains have a future in record keeping?
17. How can someone trust that the facts put on the block chain are true?

How can it be done without a third party? A third party trust is necessary to track and control that the information put on the chain is true and complete.

Interview questions (health care)

General opinion

1. What is a block chain for you? How do you understand the technology?
2. Which attributes of block chain do you consider most valuable?

Factors influencing organizations to believe in block chain

3. Do you work on a block chain project?
4. Who is using your block chain service?
5. What current problems could block chain solve?
6. What (not block chain based) alternatives can solve similar problems?
7. What benefits do you see in using a block chain?
8. Do you know of a working block chain project in your context? Are you convinced it will work?
9. What are typical barriers and difficulties in implementing block chain in health care?
10. What do you think are the biggest risks in using block chain?

After implementation

11. What happens if a patient loses his or her private key?
12. What are the costs to implement?
13. What if a block chain does not scale and fails? Can you switch back?

Can you switch from one block chain to another?

Overview and speculation

14. How would you measure the success of a block chain project in your context?
15. Do block chains have a future in health care?
16. How can someone trust that the facts put on the block chain are true?

How can it be done without a third party? A third party trust is necessary to track and control that the information put on the chain is true and complete.

Interview questions (software vendors)

General questions about the vendor

1. What clients are you servicing?

For what purposes?

2. How are you servicing users?

Is it web-based, self-hosted or a cryptosystem?

3. Who is maintaining the data integrity for your clients?

Are you storing any information of users?

4. Can average users time-stamp documents or messages on their own?

In your opinion, what is the level of complexity for time-stamping on a block chain?

5. Can anyone use your solution at any time?
6. How much does it cost to use your system?
7. What is the system's uptime?

If the site is down, can users go a different platform to verify or time-stamp?

Conceptual questions

8. What are typical barriers and difficulties in implementing block chain time-stamping for contracts and land titles?
9. What do you think are the biggest risks in using block chain?

After implementation

10. Can block chain time-stamping have any weight in solving legal issues in court?
11. Can clients have access to the data through different application? (vendor lock-in)

Speculation

12. Why do you think clients are interested in block chain?
13. What do you think is a reliable way to measure the success of your system?
14. Where do you see the block chain space evolve in the context of record keeping?

Interview questions (critics)

General opinion

1. What is so special about block chain?
2. What is a block chain for you? How do you understand the technology?
3. What efficiency do you see in using a block chain where its primary purpose is the transfer of bearer assets?
4. What benefits do you see in using a block chain?

A bearer asset becomes useless if you need to track it into a central database by a central authority and if it deals with real-world assets.

5. What do you think are the biggest risks in using a block chain?

What kind of data is safe to keep on the block chain?

Factors influencing organizations to believe in block chain

6. What are some of the main barriers blocking organizations from implementing block chain solutions?

Some believe that the whole internet can be put on the block chain. The hype is growing.

7. Why do you think organizations are interested in block chain technology?

Some of those organizations have skilled computer specialists. Aren't they aware of the risks and inefficiency of decentralized systems?

8. What would be the overall costs for a block chain implementation?

Overview and speculation

9. Do block chains have a future in record keeping and health care?
10. Do block chains have a future in business use cases?
11. How can someone trust that the facts put on the block chain are true?

How can it be done without a third party? A third party trust is necessary to track and control that the information put on the chain is true and complete.

12. How would you measure the success of a block chain project?
13. For which use case do you see block chain adoption?

Interview questions (PACCAR)

General opinion

1. What current problems could a block chain solve in manufacturing?
2. What (not block chain based) alternatives can solve similar problems?
3. Which attributes of a block chain do you consider most valuable?

Is having an ordered list the most critical attribute for the manufacturing industry? What other attributes do you find valuable?

4. What are the biggest risks in using a block chain?
5. What are the biggest barriers and difficulties in implementing a block chain solution for PACCAR?
6. What are the consequences of implementing a block chain solution in the context of a manufacturing company such as PACCAR?

After implementation

7. What do you think is a reliable way to measure the success of a block chain?

Overview and speculation

8. Where do you see the block chain space evolve in the future?