OULU UNIVERSITY OF
APPLIED SCIENCES

Mikko Huhmo

Blockchain Technology

Bitcoin as a case

Blockchain Technology

Bitcoin as a case

Mikko Huhmo
Thesis
Spring 2018
Business Information Technology
Oulu University of Applied Sciences

ABSTRACT

Oulu University of Applied Sciences
Business Information Technology

Author: Mikko Huhmo
Title of Bachelor´s thesis: Blockchain Technology, Bitcoin as a case
Supervisor: Ilkka Mikkonen
Term and year of completion: Spring 2018 Number of pages: 31

This thesis goes over Blockchain technology in the case of Bitcoin, how and what Blockchains do and what kinds of uses Blockchain might have in the future in different industries. The objective of this thesis is so that anyone, even someone who hasn't heard about Blockchain or Bitcoin, gets an understanding what it is, where it is used and what applications can it possibly be used in the future. The background knowledge for this work is mostly online and news sources, since Blockchain is a new topic and new uses are constantly arising.

Blockchain is essentially a public ledger that keeps track of any online transactions in the Blockchain network. All computers connected to this network keeps a record of the transactions and together they approve or deny data coming into the chain with certain requirements. No data can be altered without the consent of the majority on computing power in the network. Blockchain technology is a solution for many industries like banking, health care, voting, cyber security, smart contracts for many different applications, etc. However, in many industries it is still in very early stages of implementation and concrete applications are yet to be made. Altogether it saves money, time, reduces fraud, and makes many things much easier to complete or keep track of implementation is challenging.

Based on the research that were found, Blockchain technology has a much bigger use than in just virtual currencies such as Bitcoin. It can be expected be entering different industries during the next few years, such as in banking, health care, voting, cyber security, insurance, shipping, etc. These are just a few of the biggest applications that are being developed by different companies.

Keywords: Blockchain, Bitcoin, Specifications, Technology, Future Technology

CONTENTS

Glossary

Blockchain: Is a digitalized, decentralized public ledger that keeps track of all transactions made in its network. Blocks of data are added to a long chain, therefore being called the Blockchain. Can also be used not only for cryptocurrencies, but storing data and making transactions.

Cryptocurrency: A digital currency that uses cryptography (Blockchain) for security. The currency is also not centralized.

Crypto miners: People who "mine" any virtual currency with computers. They complete difficult algorithms with computers and in return get the cryptocurrency they are mining. Nowadays Graphics cards are needed since mining has gotten more and more difficult.

Distributed ledger: In other words, a distributed network. This means that the Blockchain is not on only one computer, but its distributed copies are on each computer in the network.

Hash: Processes the data of a block through a mathematical function, which results in an output of a fixed length. Using these hashes increase security since the hash is always a certain length, no matter how long or short the original message is.

Digital signature: A digital signature consists of a user's public and private key. The private key is meant for only the user, while the public key is a kind of public address where transactions can be sent.

Middleman: A person that interacts with two or more parties while making an agreement, making it safe for both sides to trade, execute contracts or send currency. Middlemen usually take a commission or a fee and usually are employed by a bank.

Node: Does quality control in the network and accepts or declines blocks that are attempted to be added to the chain according to the rules of that specific Blockchain. Nodes are essentially the computers that are in the Blockchain network

Source: Investopedia, cited 29.3.2018

1 INTRODUCTION

Blockchain is starting to become a big thing in arriving new technology. The biggest use for it right now is Bitcoin, which has risen to incredible popularity among people all over the world. However not many people understand what Blockchain really is about, and why in the case of Bitcoin, it is so popular. Blockchain keeps all transactions recorded and verifies them, making them almost impossible to hack into. It doesn't have one regulator, since everyone in the network is involved in regulating it. For someone to make any changes into the Blockchain everyone must accept them, and the best part is that Blockchain technology can be easily implemented into today's existing technology. (Hartikka 2017, cited 4.12.2017.)

Blockchain technology doesn't only stop at Bitcoin applications, but nowadays it has started to attract businesses to open its use. Banks such as OP and Nordea have stated that they will start using Blockchains in housing stocks and money transferring, since it takes fractions of the time spent on these activities today and saves money (Tivi 2017, cited 3.12.2017). Santander, one of Europe's biggest banks has launched an app to transfer money using the Blockchain, without any handling fees or middlemen (Williams-Grut 2016, cited 8.1.2018). It has the potential to overhaul the whole banking industry by taking out middlemen and handling fees, thus saving the banks millions. It could revolutionize the global banking system as we know it. Also because of how it could be incorporated onto existing technology, it has the potential to revolutionize many existing businesses. However big the affect it could have in banking other uses could be: verifying digital identities, voting, patient archives, shipping and cyber security can benefit from this as well, by reducing the number of frauds. (Beall 2017, cited 3.12.2017.) In the future Blockchain may provide a new tech explosion like the internet did in the late 90's and early 2000's.

My research methods for this thesis is to research and explain Blockchain to the everyday person, as well as to search for possible ways that Blockchains could be used in different industries. I will also include some information on how Blockchain started and how bitcoin sparked its use. Because Blockchain and Bitcoin is a new topic, a lot of the information in this thesis comes from online sources. This brings me to my question: How is Blockchain currently being used in the case on Bitcoin? How do Blockchains work and what do they do? What are future possibilities for Blockchains in different industries?

2 BLOCKCHAIN

Blockchain is a public ledger that keeps track of all online transaction securely and anonymously. It does this by keeping these actions recorded by all computers that are connected into the Blockchain. Essentially every user authenticates the transaction and approves it. This way no single person can technically alter or "cheat" the system. It would require all computers connected to the Blockchain, which are recording data, to alter its data for it to become "real". Blockchain is also decentralized, meaning that no governments, authorities and single locations are used. Being decentralized and because the data is scattered by many computers they keep Blockchain protected. (Hartikka 2017, cited 4.12.2017.)

2.1 Technology behind Blockchain

Blockchain technology is a new way of combining already existing technologies, such as public and private keys, digital signatures, peer to peer networks and distributed ledgers. Blockchain is a combination of all these.

The Blockchain is very secure considering that information can be shared, produced and maintained completely decentralized (distributed ledger). Everyone who joins the network gets a copy of the network via the distributed ledger. In this big network everything is accepted or denied using a consensus procedure. These procedures are conducted by "nodes" which control the quality of data, but also accepts or denies information depending if it is according to the rules of the Blockchain. When the network agrees that data is accepted it is then made into a block. The peer to peer network (distributed ledger) decides between certain intervals if a block is added to the chain. (Rissanen 2018, cited 18.2.2018.)

Blockchain is a technology based around everyone in the network. For example, in figure 1 below, if someone wants to send money to a person, they create a "transaction block", which then is shown to everyone in the network. When all the users approve the transaction, the block is then added to the other blocks that other people have made doing these kinds of transactions. Blocks contain a digital signature, timestamp and other relevant information. (Baurle 2017, cited 3.12.2017.) The blocks create a long chain, therefore getting the name "Blockchain. The root of the chain dates to the very first block ever created. If the block is not approved by the network or does not have a corresponding number to the previous block, it is not allowed to join the chain.

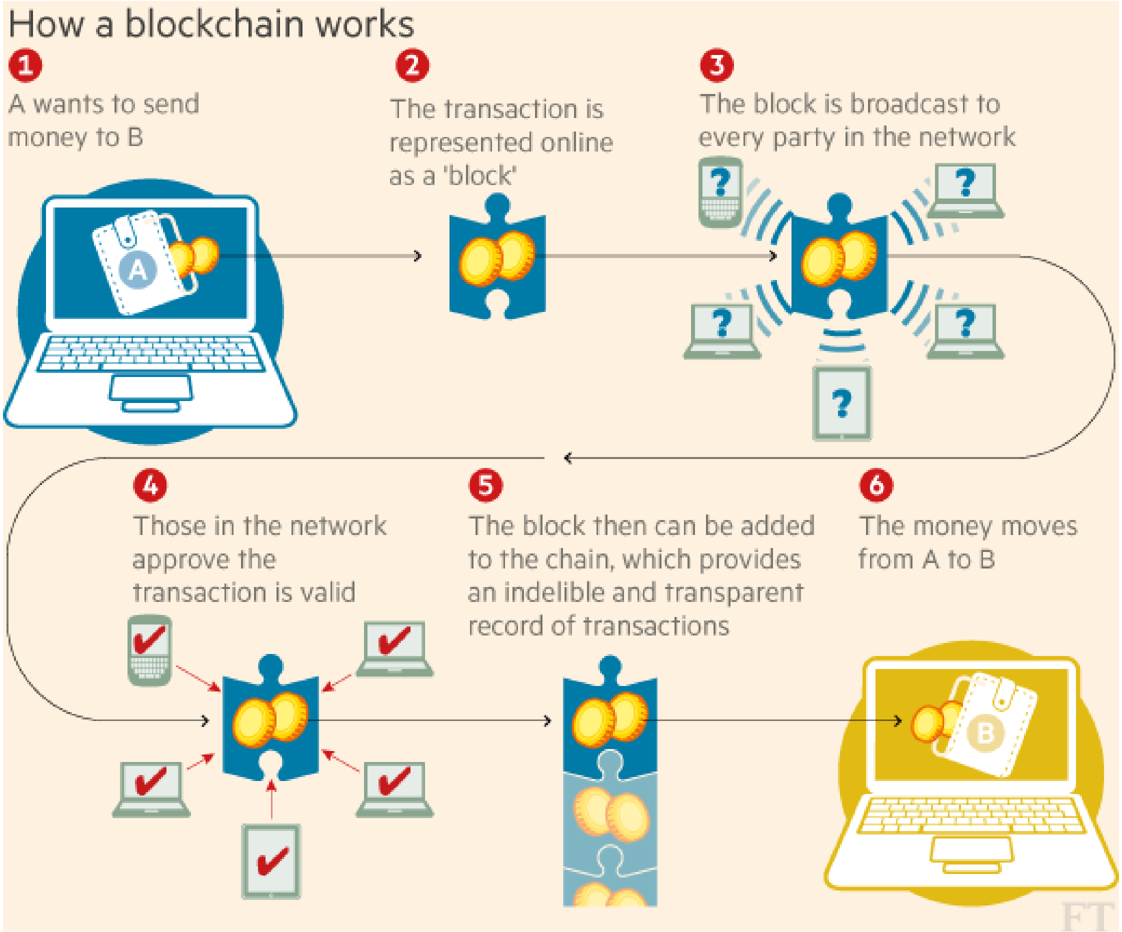
How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B
FT

Figure 1. How a Blockchain works (AID:Tech, cited 3.12.2017)

2.1.1 Distributed Ledger

The data in the Blockchain is stored in a distributed ledger, which means it is spread across many different users in different areas, erasing a central figure to keep track that the system is under control. The information is securely saved using cryptography and only accessible using keys and signatures. Because the information is stored in distributed ledgers, it is very hard to attack using malicious software. Each different network has its own rules that are being followed, but in every case for any attack to be successful, each copy of the distributed ledger would have to be targeted at the same time. (Investopedia 2018, cited 16.2.2018.)

There are four different types is distributed ledgers. These are permission less public, permission less private, permissioned public and permissioned private. Each of these ledgers are used in different types of environments and have different ideologies.

Permission less public's central idea is proof of work. In Bitcoins case it uses this ledger and the users mining bitcoin serve as a kind of validator of the proof of work. Also, anyone can download the software and validate transactions.

Permission less private's idea is that the Blockchain is private and closed from the public. In this type of ledger there is no mining involved like with the case of bitcoin.

Permissioned public means that information storage is limited, but everyone can read them. In this ledger, a user that validate transactions must meet some requirements. These requirements may be a ID card.

Permissioned private ledger is the most limited of these four and is used inside companies. Only the users inside the company can read and store data in the Blockchain. (Rissanen 2018, cited 16.2.2018.)

While permission less public ledgers are anonymous and possible malicious, permissioned private and public ledgers have users identified and trusted. It doesn't use the proof of work consensus, but rather a voting/ multi-party system. This means they vote on every data put into the Blockchain. These ledgers are lighter, faster, use less energy and enable finality. The Blockchains that use these ledgers have much shorter transaction times compared to bitcoin, in the milliseconds. In return, these ledger types can cut down transaction costs dramatically and have more transparency. (BlockchainHub, Blockchains & Distributed Ledger Technogies, cited 16.2.2018.)

Because of bitcoins huge spike in its popularity transaction approval takes around 10 or more minutes. Its proof of work will become a problem when all bitcoins have been mined, since who owns the most computing power in the whole network controls Bitcoin. (BlockchainHub, Blockchains & Distributed Ledger Technogies, cited 16.2.2018.

2.2 Block Specifications in the Case of Bitcoin

Each block consists of a digital identity, peer to peer network and the Blockchains protocol (what the block needs). Each user has a public and private key, which together, create a user's digital signature. The public key is a key consisting of numbers and letters and is used to identify another user. In return the private key is personal and knowledge of the user themselves. When sending cryptocurrency this public key is used to send and receive. (Bauerle 2017, cited (8.1.2018.)

The other half of the digital identity, the private key, is a kind of password. It is meant to be known only by the user and is also consisted of numbers and letters. The private key (only visible to you) generates a public key (visible to everyone). One difference compared to the public key is that the private key is somewhat longer. If the private key stays private there should not be a way for anyone to get into your Blockchain wallet. Shortly said "you sign the cryptocurrencies you send to others using a Private Key" (Di, 2017, cited 8.1.2018). This creates your own digital signature on blocks going into the Blockchain. In figure 2 below it can be seen that both private and public key are used to create a block into the Blockchain.

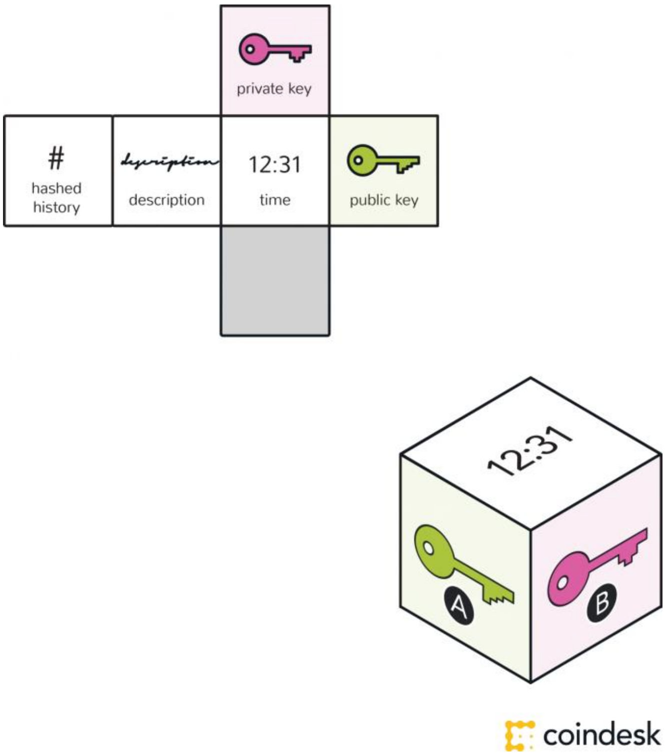

Figure 2, How does Blockchain technology work? (Coindesk, cited 8.2.2018)

The peer to peer network is the network created by other users. The transactions made in the network are recorded by all other devices there. All the devices then check the transaction, in this case bitcoin, and verify it.

When verified and accepted by all devices the Blockchains protocol then makes a block out of this information. A digital signature (created by a public and private key), timestamp of when the transaction was made, in sometimes a description is provided, alongside with a hashed history. The hashed history, in bitcoins case, means that SHA 256 is used. This creates a 256-bit hash of the data inside the block. Every message is put into a hashed format, which means the data or message in that block is input into a fixed hash length. This is a “code” of a fixed length that when deciphered reveals what data the actual block holds. Then when another block enters the chain it always includes the previous hash (data) of the previous block like shown in figure 3 down below. (Rosic 2017, cited 8.1.2018.)

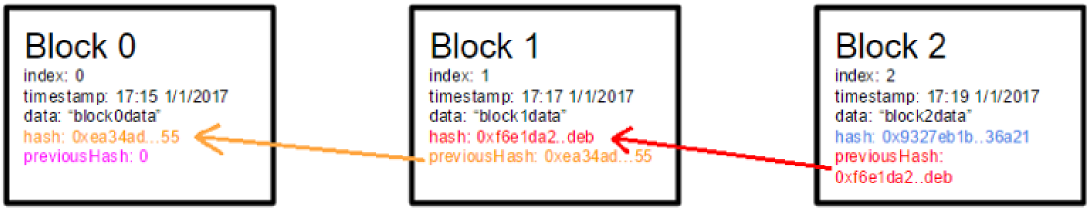

Figure 3, A Blockchain in 200 lines of code (Medium, cited 8.2.2018)

The components inside the network are divided into 3 main parts: the user's identity, the big network of people that keeps the records/transactions and the Blockchains protocol (digital signature, timestamp, other information. These three components build the Blockchain network.

2.3 Industry Uses for Blockchain

Though the biggest use right now for Blockchain is the virtual currency Bitcoin, Blockchains can be used for a variety of different applications. They can be used in many industries, such as voting systems, real estate, shipping, cyber security, banking and so on. Today, Blockchain technology is not yet used for many of these commercially, but it has created a lot of interest on how it could make these industries easier. One of the biggest, banking, has sparked interest due to possible billions in savings, voting could reduce fraud and violence, shipping could reduce money, time and easiness. All in all, saving money, time, increasing safety are the three biggest factors. (Beall 2017, cited 8.1.2018.)

2.3.1 Banking and other Contracts

Banks have started to explore the use of Blockchain. The thought to reduce transaction costs is a big deal to them. Santander, a well-known bank estimated the annual savings of taking Blockchain into use at around 20 billion dollars (Williams-Grut 2016, cited 8.1.2018). Using Blockchain technology in banking would eliminate middlemen costs and other handling fees from the user and from the bank. However, for Blockchain use to succeed in banking, it would have to be taken into use around the world to help reduce the risk of failure. Transactions generally can take up too many days before being completed today, but with the help of Blockchain they could be completed within hours or even minutes/seconds and without any huge costs for the user or bank. (Beall, 2017, cited 19.1.2018.)

However, a big risk for banks is Blockchains security. If it were to fail, the costs would be enormous. Despite the potential risks, it wouldn’t only help banks reduce costs, but also create new products/ services and help to keep records easily (Accenture Digital 2017, cited 8.1.2018). A whole new “digital banking” era would start and, according the George Beall, a potential 2 billion who don’t have a bank could access it via smartphone. This would be a major source of income for banks. Bitcoin has not experienced even a second of downtime so this would provide a very stable platform for the user and bank. (Beall, 2017, cited 19.1.2018.)

Real estate businesses have started to change into digital format in Finland. One of the possibly uses would be the use of Blockchains. According to Tero Lehto for Tekniikka & Talous newspaper, all the documents needed when dealing with houses (certificates, quality inspection certificates, landlord reports, etc.) could be easily accessed via Blockchain. This would make the seller of the house in charge and cut out all the middlemen. They would be able to start, control and end the whole sale via the web. Although a plausible solution candidate, the Blockchain still has its problems for such a large use, such as this. The network isn't yet big enough or have enough power to handle such load. (Lehto, 2017, cited 8.1.2018.)

Smart contracts would also be a big application for the use of Blockchains in banks and apartment deal making. It would be a pivotal part of managing different kinds of agreements, accounts and storing data of an application. Smart contracts make it so that the agreements made are secure and only accessible by the ones who are a part of it, by digital signatures. In Bitcoins case, it was the first one to utilize this, but only with currency. (Hertig, 2018, cited 23.4.2018.)

2.3.2 Voting

Voting is yet another way to utilize Blockchains. Because Blockchain provides an impenetrable system and past events can only be altered if the majority allows it, it could provide a see-through system for the public as well. This could reduce several riots and deaths that have happened like in Honduras and Kenya in late 2017, where dozens of people got killed while stating that the elections weren't fair. The voters believed that some voters could not vote normally, votes being recounted and other manipulation. (Hochstein, 2018, cited 24.4.2018.)

Shortly after this, on March 13, 2018, Sierra Leone elections scouted for possibly use of Blockchain voting using the Agora companies Blockchain, but did not yet commit to it. Russia on the other hand already started a program called “Active Citizen”, in 2014, where citizens could vote on different polls regarding the city. As of late 2017 it incorporated using Blockchain technology to make the results publicly auditable and to gain citizens trust on voting. The new Blockchain system places any votes into a ledger containing all the votes that are spread across a peer-to-peer network. As Active Citizen responds, “It will guarantee that the data will not be lost or altered by someone after the vote was casted so there is no chance for fraud or third-party interference". (Hochstein, 2018, cited 24.4.2018.)

Each voter would be verified by the Blockchain and have their own public and private ID. Using these ID's, they would remain totally anonymous, but also very secure. The Blockchain could possibly be a permissioned public Blockchain, where people could cast their vote with some pre-requirements and then follow how the voting is going and verify any results. There would be no confusion or frauds happening. No "false" votes and multiple votes from one person could be done because the Blockchain would not allow it because of its rules. When the votes would be tallied it would be done very transparently and fairly, since the results can't be altered. The voters wouldn't have to travel to the voting place or wait in lines. Using Blockchain technology would also reduce the number of recounts, legal costs, and corruptions. (Meylan & Runde 2018, cited 19.4.2018.)

This is the case in Estonia. "I-voting" has been used in nationwide elections since 2007. It was the first country to do so already in 2005 with internet voting, but moved to use Blockchain technology in 2007. Voting is done by using the user's personal id card to cast a vote. This can be done anywhere and a person can vote many times if they decide to change their vote. If they vote more than once, the previous vote is always canceled, eliminating the possibility for forcing votes. For Estonia using this kind of voting system in elections have saved over 11,000 working days. I-voting eliminates the need for voting booths and provides clearness for the people by eliminating fraud. (E-Estonia 2018, cited 5.7.2018.)

2.3.3 Health Care

Health care would be a big sector for Blockchain technology. Electronic patient records would remain like they normally do, however digital fingerprints would be put on all patient records which could then be accessed via the Blockchain. This would generate an event log, so it would be visible which doctor, nurse or otherwise unrestricted person would have looked or altered any information from an electronic patient record. That creates a see-through system, much like in the case of voting. (Rissanen 2018, cited 23.4.2018.) This is already being used in Estonia, which came the first country to start using Blockchain in their health care system. E-services, as it is referred to, is available to everyone who has visited a doctor in Estonia. They can log in via the web using their own electronic ID-card. The data is kept secure, but also open to authorized personnel. For example, during an emergency the doctor can use a patient’s ID and see “time critical information, such as blood types, allergies, treatments, on-going medication or pregnancy”, as stated in Estonia’s official website. Almost all prescriptions, billings and health data is electronically handled and accessed via the KSI Blockchain, which Estonia uses. The KSI Blockchain is specifically been designed in Estonia for government use and “makes sure networks, systems and data are free of compromise, all while retaining 100% data privacy” (E-Estonia 2018, cited 27.4.2018). The KSI network has many more technologies added to it than Bitcoin. (E-Estonia 2018, cited 27.4.2018.)

2.3.4 Shipping

This would also be the case for shipping. Products could be overseen where they are produced and past travels before it arrives at its destination. This would help reduce the number of counterfeit products and provide a sense safety for all parties involved (Beall 2017, cited 19.1.2017.)

IBM researched how Blockchains could be used for the global flower market estimated to be around 105 billion dollars. Around 700,000 metric tons of flowers are shipped every year and one shipment may demand up to 30 different organizations to fill out forms. If any forms are late, misunderstood or lost the shipment will result in being late. The solution IBM is working on is a digitalized version using Blockchain technology. It would use smart contracts as a big part to speed things up. These are contracts that are made by opposing parties and written as code and added to the Blockchain. All the information inside that smart contract is only known by the parties involved, but otherwise the coded contract is public knowledge. Then when an event such as payment or a certain date occurs the contract accomplishes the task it was supposed to do. This is shown in Blockgeeks figure 4 below. (IBM, 2017, cited 27.4.2018.)

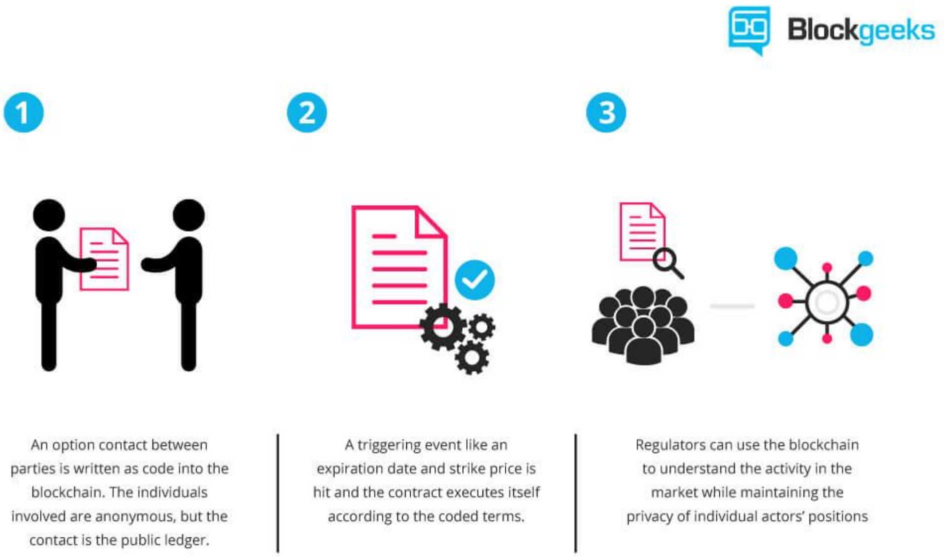
Blockgeeks
1
2
3
An option contact between parties is written as code into the blockchain. The individuals involved are anonymous, but the contact is the public ledger.
A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.
Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions

Figure 4. Smart contracts: The Blockchain Technology that will replace Lawyers (Blockgeeks, cited 27.4.2018)

This would make the process many times faster, easier and transparent for all parties involved. It would result into reduced fraud and errors, reducing delays caused by paperwork, reducing waste and cut down on courier costs. According to IBM this would increase worldwide GDP's by almost 5% alone and trade volume by 15%. (IBM, 2017, cited 27.4.2018.)

2.4 Blockchain Promises and Security

Blockchain has some difficulties and complexions concerning its success. The network where Blockchain would be used needs to have many users to be secure as well as be utilized to its full potential. However, like seen in figure 5 below, because the Blockchain is distributed among many computers there is no single point of failure, thus making it hard to hack into. The biggest flaw is perhaps the "51% attack" where if most of the computers were to tell a lie it would be treated as the truth. This "rule" cannot be changed since it was made in to system. (Bauerle, 2018, cited 22.3.2018.)

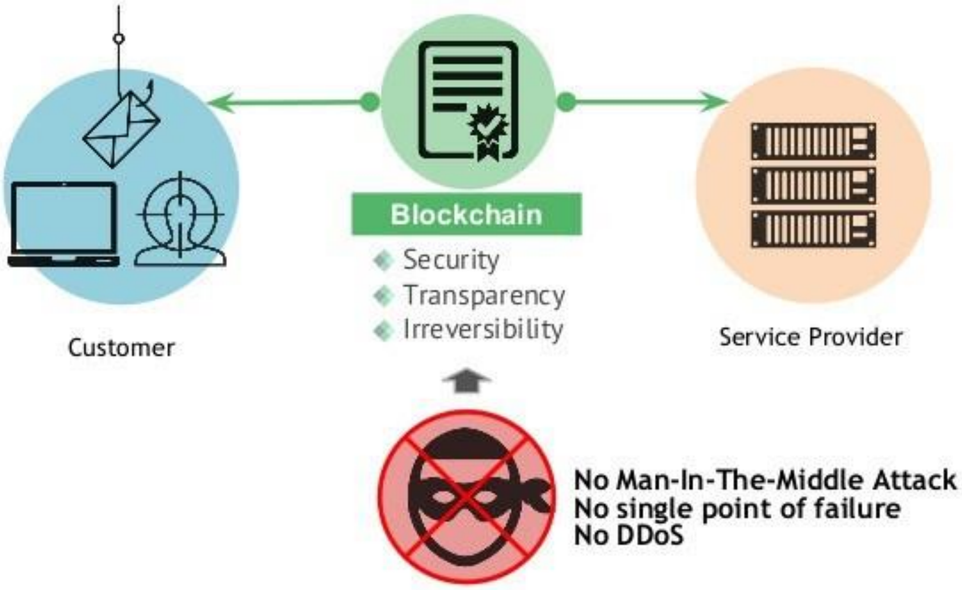

Figure 5. The four Pillar of Blockchain technology (Ricktopia, Cited 22.3.2018).

In the beginning of the Blockchain, first used in bitcoin, it had no big transaction costs. However, since now that the user base as exploded the transaction costs have risen very high. The Bitcoin Blockchain can process around 7 transactions a second, while others might be capable of much more. Lastly data put into the Blockchain needs to be accurate so that past events documented can be trusted. (Bauerle, 2018, cited 22.3.2018.)

2.4.1 Risks Using Blockchain now and in the Future

There are many risks of using Blockchains now and in the future. Many of them are still many years away from possible happening, but are viable risks. Possible risks like: Quantum processors, owning majority of processing power, most computing power in one country, not having enough processing power to increase active users and that illegal material resides in the Bitcoin Blockchain.

The Blockchain records everything that is put into it. Even though nodes go through every "transaction", if the data is according to the Blockchain rules it can include in the chain, there it remains forever. Very recently German researchers discovered that of the 1600 files in Bitcoins Blockchain, at least 8 of them had sexual content, containing links to child abuse subject and to dark web services. Because every user in the Bitcoin Blockchain downloads a copy of the Blockchain it can be make the use and possession of the Bitcoin Blockchain illegal. If countries rule, that using Blockchains because of this, is illegal then it could have major impacts on the computing power distribution. (Gibbs, 2018, cited 23.4.2018.)

The distribution of computer power resides mostly in China. According to Kaspersky, 81% of Bitcoins mined came from China. One reason is it' slow energy costs and cheap labor. However, since this amount of computing power comes from one country it could have risks if many of the mining pools were to merge, thus then holding most of the computing power. From all the mining pools 4 of the largest own over 50% of the computing power, all in China, which would make this not that hard to do. (Melanov, 2017, cited 23.4.2018)

Another problem for right now is that the Blockchain network, at least of Bitcoins case, doesn't have enough computing power to raise the number of active users. The Bitcoin Blockchain can process seven transactions a second and Bitcoin transactions are recorded only every 10 minutes. While many users wait around an hour to make sure the transaction goes though, because of possible rollbacks. This needs to be increased dramatically to make a possible use for everyone. (Melanov, 2017, cited 23.4.2018)

The first Quantum processors are speculated to come to market in around 10 years and they pose a real risk for the future of existing Blockchains. Google speculated that they would be millions of times faster than today's processors and getting a hold of one today would break the Blockchain. The owner of that processor would immediately gain control of the Blockchain. Even though they scientists have not yet been able to create one, speculations have been made that we would only be 10 years away from them. A quantum processor allows electrical circuits to be in a 0 and 1 simultaneously compared to processors today that can be only either one at a time. For example, in the case of Bitcoin this would allow them to easily complete difficult calculations and algorithms and it could break digital signatures, which would mean forging transactions and stealing coins from others. (Fratto, 2018, cited 23.4.2018).

2.4.2 The 51% Attack

The 51% attack means that if most of computing power was contained by a single person or group, they could then control the whole Blockchain. In the case of bitcoin, the controlling person could alter existing blocks, control incoming blocks, deny other people from accessing blocks, reverse transactions, etc. Because big miners control a large portion of the computing power, they possess the most influence on the currency. This essentially would lead to the end of bitcoin if they would use this advantage negatively. (Rocky, 2016, cited 22.3.2018.)

This happened in 2016 with Krypton, another cryptocurrency. This involved overpowering the network with over 51% computing power to roll back transactions and spending the coins. This made it so that they received double the coins. The attackers also did a DDoS (distributed denial-of-service attack) to the nodes in Krypton's Blockchain, which made them have even more power over the network. The cryptocurrency ultimately survived the attack and made changes to its service, so that withdrawals of the currency would have to go through 1000 confirmations, preventing the same kind of attacks in the future. (Rocky, 2016, cited 22.3.2018.)

51% attacks in private Blockchains, like in companies, would not be so common. Companies use private Blockchains (permissioned). This means the owner of the Blockchain gives permission to only certain people he trusts/ knows. Though like in any trusted procedures anyone could misuse their positions, it is up to the owner to manage the persons inside the Blockchain. (Rissanen 2018, cited 22.3.2018.)

2.4.3 How to Prevent 51% Attacks

The 51% attack could happen in any Blockchain based system. However, since nowadays the biggest use for Blockchains is virtual currency it could pose a big problem. If a 51% attack were to happen in a bigger network like Bitcoin, "One of the things a 51% attacker can do is prevent any transactions or new blocks from anybody besides themselves from being accepted, effectively stopping all payments and shutting down the network, as a chief scientist Gavin Andersson, at Bitcoin states. Despite it being very bad, he also says that it would be easy to defend against since the confirmation requests could be raised and the attacker would have to maintain most of hashing power and have a ton of old bitcoins to keep with DDoS attacks. Basically, it would just be a temporary case and would be fixed. However, being only temporary it wouldn't be good publicity and code has already been made in case of that. The community also keeps a precise measurement of the current computing power. The biggest being BTC.com having around 29% market cap as of 23.4.2018, according to the official Blockchain website (Blockchain 2018, cited 23.4.2018). In 2014 the mining pool Gnash controlled around 42-47% of the total network hash rate, which lead to the community bringing the matter up and confronting them. Gnash stated it didn't want to own more than 51% of the hash rate simply because they would not benefit from it, they would become everyone's enemies and it would have risked their own investments. (Quentson 2014, cited 23.4.2018.)

2.4.4 Blockchain Promises

Blockchain technology promises the users several guidelines and rules to follow:
1st: Data saved into the Blockchain is immutable and the transaction history cannot be changed after it has already happened.
2nd: Data containment is totally distributed among all the computers in the network and all the information in the Blockchains is backed automatically.
3rd: Handling information is collaborative and different operators trust is coded into the system.
4th: The data transmission has no middlemen. It provides a way to conduct matters that require trust without a trusted 3rd party (such as banks).
(Rissanen 2018, cited 22.2.2018.)

These 4 "rules" create the backbone of any Blockchain but can be overturned by the 51% rule.

Blockchain, in industry use, essentially promises to take out middlemen, creating more transparency, reduce fraud and payment errors, protect critical infrastructures from cyber-attacks, share information faster/ cheaper, and should reform all economic life. Simply put, it would create a whole new business.

Taking out middlemen would save companies tremendous amount of money, for example even taking out a 1% transaction fee in a big bank would result in millions being saved. Though jobs would be lost, but they would be replaced by new jobs concerning the Blockchain. Taking

Blockchain into use would also create transparency on what information user's look at, seeing where shipments are/have been during each step of the shipment, etc. This would erase frauds and other payment issues. Lastly because Blockchains are virtually impenetrable with today's technology it would cut down on cyber-attacks with the added easiness of sharing and storing data. (Rissanen 2018, cited 22.3.2018.)

3 BITCOIN

Bitcoin was the first cryptocurrency made and the biggest user of Blockchain today. It was created by so called “Satoshi Nakamoto” in August 2008. The name “Satoshi Nakamoto” is made up alias and people still don’t know who the real person or group behind this idea really is, but many speculations have been made. Satoshi came up with the idea of Bitcoin, using Blockchain technology, in 2008, after the collapse of the U.S. housing market. As the creator Satoshi Nakamoto took 20% of all Bitcoins in distribution currently for him or them. After creating it he or they spread out a paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” to others and so word spread. Then after around half a year, in January 2009 bitcoin became accessible to mine through a software program. It could be “mined” otherwise known as processing complex algorithms by just using a computer CPU. Compared to today, it is no longer worth to mine because how much power and resources you need to stay cash flow positive. (Bernard 2017, cited 25.1.2018.)

Before 2010 Bitcoin really didn’t have any purchasing power, but in 2010 the “so called” first bitcoin transaction was made. It consisted of trading 10000 bitcoin for another person so that they would get two pizzas’ in return. Back then one bitcoin was 0, 08$ compared to the price of today (25.1.2018) of 11,403$. This paved the way for the next big marketplace for Bitcoin, called Silk Road. (Kostarelis 2017, cited 25.1.2018.)

Silk Road launched in 2011 and founded by Ross Ulbricht. It was an online marketplace for illegal drugs and other things. The site had rules, despite being illegal, such as selling anything that’s purpose would have been to hurt someone would be banned. However, buying drugs was as easy as any other online store, only here bitcoins were used together with an anonymous network called TOR. This way tracing back to the buyer would be made very hard. Due to this illegal marketplace operating for around 3 years, before being shut down in 2013, people got the idea bitcoin was only used by criminals. However illegal activities were used, Silk Road is a very important piece of bitcoins early history. Today bitcoin has its own ATMs, used in hundreds of websites, government starting to recognize it as a currency, etc. (Chen 2011, cited 25.1.2018.)

After 2011 several hundred of rivaling cryptocurrencies entered the market, each with their own take on what they are planning to create. However, Bitcoin being the largest, it would influence the price of all the other smaller currencies. In 2013 the first Bitcoin crash came, where the price dropped from 1000$ to 300$, but today, it has risen to over 10,000$, despite having multiple crashes on the way. (Marr, 2017, cited 25.1.2018.)

3.1 Technology behind Bitcoin

Bitcoin uses Blockchain technology behind the scenes. Bitcoins are stored in a digital wallet created by the user and is referred to by their public key, the user can get into their wallet with their private key. Just like Blockchain when some amount of bitcoin is transferred to someone it creates a block onto the Blockchain to keep data on every transaction made. Every transaction is anonymous, only referring to a public key. Then, like in Figure 1, it is verified by other computers in the network and confirmed. (The Economist 2015, cited 26.1.2018.)

Bitcoins are mined by computer CPUs and GPUs that are connected to the mining software. There are bitcoin blocks released every 10 minutes and after being released anyone mining can have a chance to find that block. However, every day the mining difficulty increases. To make a comparison, when bitcoin started in 2009, the difficulty was 1. Now the difficulty is 2,603,077,300,219 (Bitcoin Block Reward Halving Countdown, 2018). It is so high that normal computers don’t have enough power to find them anymore like they used to in the beginning. Nowadays there are companies that mine with thousands of computers and graphics cards to find these bitcoin blocks. For example, an aircraft hangar in Boden, Sweden is being used to mine bitcoin. As seen in Figure 6 below, it stores over 45,000 computers, trying to solve mathematical puzzles. Since only one computer in the world can find a single block the bitcoin there is big competition. This number of computers uses nearly around the same amount of electricity as 135,000 homes in the U.S. (The Economist 2015, cited 26.1.2018.)

Figure 6. The magic of mining (The economist, cited 26.1.2018)

3.2 ICOs and Token Sales

Blockchains are the basis in all cryptocurrencies. They might differ in the in different forms, such as permissioned, permission less, private and public Blockchains. For example, Bitcoin uses a permission less public ledger so that anyone can mine or make transactions, while the cryptocurrency Ripple is permission less and private, where the Blockchain is private. They all have in common that the currency is away from any government ruling. (BlockchainHub, 2017, cited 29.3.2018.)

ICO's or initial coin offerings are ways companies raise investment from supporters, in return for giving out their cryptocurrency. The companies are essentially preselling the coin and using the money gathered from this to continue their project. People that support the project will invest early to have more of a chance to get a better return. The coins act as a sort of currency which can be sold at any time, and fluctuate as the project moves forward, gains popularity or news breaks. There are hundreds of coins, each having a different kind of project. However, because the Blockchain based token sales have little to no regulations set by governments it can have insecurities. (BlockchainHub, 2017, cited 29.3.2018.)

The company provides a “whitepaper” which has a business model, coin distribution and supply, price of a token, a timeline and target budget for the funds. Potential investors can read it and get a sense of the project. Often it promises many things and the image of that project can get a huge gathering of investments. (BlockchainHub, 2017, cited 29.3.2018.)

4 CONCLUSION & DISCUSSION

Blockchain is changing the world in ways yet not known by many people. Many people have heard about Bitcoin, but don’t understand what lies beneath it. Some people believe that Bitcoin is just a pyramid scam and therefore shouldn’t be taken seriously. The truth is that Bitcoin is not the most valuable thing about the cryptocurrency, instead it is the technology that lies underneath it. That technology is Blockchain. It can be used to save costs in transactions and getting rid of middlemen, make data storage easier, increasing cybersecurity, creating new jobs, saving time and money, etc. Theoretical uses for the Blockchain are essentially endless and more uses for it will grow in the future.

The main questions that the thesis is trying to give answers to are:

How do Blockchains work, what do they do and what risks are involved?
How is Blockchain currently being used in the case on Bitcoin?
What are future possibilities for Blockchains in different industries?

As a result, to these questions, this thesis explains Blockchains to people who are yet not familiar with the subject. Blockchain is essentially a public ledger that keeps track of all online transaction securely and anonymously. It is a distributed network and all computers that are connected to it have a copy of the Blockchain, including all transactions made. These computers, or nodes as they are called, verify each transaction with a set of pre- requirements and determine if it can be added to the chain or denied from it. Blockchains are not only for virtual currency use, but can be implemented into different types of businesses such as banking, health care, voting, smart contracts, shipping, etc. It will save time, money and provide a clear, see-through picture for everyone. Also, less frauds will occur because of Blockchain security measures. However, since Blockchain is evolving at a high rate, many more industries may benefit from this as well in the future.

In the case of the virtual currency Bitcoin, it was the first application to use Blockchain. It works the same way as explained above, but also uses a virtual wallet to store Bitcoin. These wallets are very secure and have public and private keys to back them up. Bitcoins are mined with computers graphics cards, completing difficult algorithms and everyone who is mining gets a chance to “find” a new block containing Bitcoin every 10 minutes. Bitcoin however, is only one-way Blockchain is used and it would work with the same principle with other applications like banking, but altered a little to make them work better with that application. However, with everything there are always risks. The biggest Blockchain, used in Bitcoin, still can't handle a larger active user base and that is really holding the technology back. Because of this big user base transaction times have gotten slower and more expensive. Also, possible loop holes like the 51% ownership of all computing power in the network and new technologies like quantum processors in the future may pose risks. These are some of the issues that must be fixed before incorporating Blockchain with bigger markets such as health care, banking and voting.

My findings from this thesis were much bigger that I had expected. Though I had prior knowledge of the topic, it blew me away to see how Blockchain really works and what kind of uses it might have in the future. At first, I only thought about Bitcoin being a new thing and that it could be used in the future, but didn't really think about how it works or that it could be even used in other applications.

While researching and going behind the scenes of the Blockchains, I certainly believe they will become a part of our future in our everyday things, such as banking, health records, voting, identity, etc. It is already being introduced by different banks such as Santander and OP, using it with voting in Russia and Estonia to reduce fraud, violence and to save time and around a million health records in Estonia are based on Blockchain technology. They all have same applications as the original Blockchain used in Bitcoin, however some disadvantages might have been erased. Also since the Blockchain promises tamper proof data, data is totally distributed and distribution of data is disintermediated. It is potentially a lot better solution that can be implemented on existing infrastructures. There is no limit for what Blockchain couldn't accomplish in the future.

REFERENCES

Accenture Digital. 2018. Join the Blockchain Party. Cited 8.1.2018, https://www.accenture.com/fi-en/insight-blockchain-technology-how-banks-building-real-time

Baurle, N, 2017. How does Blockchain technology work? Cited 3.12.2017, https://www.coindesk.com/information/how-does-blockchain-technology-work/

Baurle, N, 2018. What are Blockchain's Issues and Limitations? Cited 22.2.2018, https://www.coindesk.com/information/blockchains-issues-limitations/

Beall, G. 2017. How Blockchain will change major industries. Cited 9.11.2017, https://thenextweb.com/contributors/2017/11/09/how-blockchain-will-change-major-industries

Bernard, Z. 2017. Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator. Cited 25.1.2018, http://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12?r=US&IR=T&IR=T/#in-2008-the-first-inklings-of-bitcoin-begin-to-circulate-the-web-1

Bitcoin Block Reward Halving Countdown, 2018. Cited 25.1.2018, http://www.bitcoinblockhalf.com/

Blockchain. 2018. Hashrate Distribution. Cited 23.4.2018, https://blockchain.info/pools

BlockchainHub, 2018. Blockchains & Distributed Ledger Technologies. Cited 29.3.2018, https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

BlockchainHub, 2017. ICOs – Initial Coin Offerings – Infographic. Cited 29.3.2018, https://blockchainhub.net/blog/infographics/initial-coin-offerings/

Casey. M, 2016. AID:Tech. Could Blockchain technology help the world's poor? Cited 3.12.2017, https://aid.technology/could-blockchain-technology-help-the-worlds-poor/

Chen, A. 2011. The Underground Website Where You Can Buy Any Drug Imaginable. Cited 25.1.2018,
http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160

Derin, C. The four pillars of Blockchain technology. Cited 22.3.2018,
https://richtopia.com/emerging-technologies/four-pillars-blockchain-technology-part-1

Di, L. 2017. Why Do I Need a Public and Private Key on the Blockchain? Cited 8.1.2018,
https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76

E-Estonia. 2018. KSI Blockchain. Cited 27.4.2018,
https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/

E-Estonia. 2018. E-health records. Cited 27.4.2018,
https://e-estonia.com/solutions/healthcare/e-health-record/

E-Estonia. 2018. I-voting. Cited 7.5.2018,
https://e-estonia.com/solutions/e-governance/i-voting/

Fratto, N. 2018. Commentary: This New Technology Will Crack the Blockchain Like an Egg. Cited 23.4.2018,
http://fortune.com/2018/01/31/commentary-this-new-technology-will-crack-the-blockchain-like-an-egg/

Gibbs, S. 2018. Child abuse imagery found within Bitcoin's Blockchain. Cited 23.4.2018,
https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content

Hartikka, L. 2017. A Blockchain in 200 lines of code. Cited 9.11.2017,
https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54

Hertig, A. 2018. How Do Ethereum Smart Contracts Work? Cited 23.4.2018,
https://www.coindesk.com/information/ethereum-smart-contracts-work/

Hochstein, M. 2018. Moscow’s Blockchain Voting Platform Adds Service for High-Rise Neighbors. Cited 24.4.2018,
https://www.coindesk.com/moscows-blockchain-voting-platform-adds-service-for-high-rise-neighbors/

IBM. 2017. Blockchain Supply Chain Infographic: The Paper Trail of a Shipping Container. Cited 27.4.2018,
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XI912347USEN

Investopedia. 2018. Distributed Ledgers. Cited 16.2.2018,
https://www.investopedia.com/terms/d/distributed-ledgers.asp

Kostarelis, S. 2017. The first-ever Bitcoin transaction was used to buy two pizzas – today, it’s worth $150 million. Cited 25.1.2018,
https://www.techly.com.au/2017/12/05/first-ever-bitcoin-transaction-used-buy-two-pizzas-today-worth-150-million/

Lehto, T. 2017. Lohkoketju myy asunnon ilman paperisotaa. Cited 8.1.2018,
Helsinki, Tekniikka & Talous.

Marr, B. 2017. A Short History of Bitcoin and Crypto Currency Everyone Should Read. Cited 25.1.2018,
https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/2/#4b491ba0533c

Meylan, P. & Runde, D. 2018. Blockchains Will Change the Way the World Votes. Cited 19.4.2018,
https://www.csis.org/analysis/blockchains-will-change-way-world-votes

Melanov, A. 2017. Six Myths about Blockchain and Bitcoin: Dubunking the effectiveness of the technology. Cited 23.4.2018,
https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/

Quentson, A. 2014. 4 Lines of Defence Against a 51% Attack. Cited 23.4.2018, https://www.ccn.com/4-lines-defence-51-attack/

Rissanen, T. 2018. Blockchain – lohkoketjut ja distributed ledger -teknologiat. Cited 16.2.2018, https://www.brighttalk.com/webcast/14223/304731

Rocky, 2016. Krypton recovers from a new type of 51% network attack. Cited 22.3.2018, https://cryptohustle.com/krypton-recovers-from-a-new-type-of-51-network-attack

Rosic, A. 2017. What is hashing? Under the Hood of Blockchain. Cited 8.1.2018, https://blockgeeks.com/guides/what-is-hashing/

Rosic, A. 2017. Smart contracts: The Blockchain Technology that will replace Lawyers. Cited 27.4.2018,
https://blockgeeks.com/guides/smart-contracts/

The Economist. 2015. The magic of mining. Cited 26.1.2018, https://www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic

Tivi. 2017. HS: Suomalainen jättirekisteri siirtyy lohkoketjuun – ”Kivikaudelta digiaikaan”. Cited 3.12.2017,
https://www.tivi.fi/Kaikki_uutiset/hs-suomalainen-jattirekisteri-siirtyy-lohkoketjuun-kivikaudelta-digiaikaan-6685497

Williams-Grut, O. 2016. Santander is letting staff use the tech behind bitcoin to send money to each other. Cited 8.1.2018,
http://www.businessinsider.com/santander-develops-blockchain-international-payment-app-with-ripple-2016-5?r=UK&IR=T&IR=T