Accounting, Auditing and Blockchain

Interviews with Finnish auditors about blockchain

Niclas Gröndahl, 35792

Supervisor: Ralf Östermark

Faculty of Social Sciences, Business and Economics

Åbo Akademi University 2020

Table of Contents

1. Introduction 1
   1.1. Problem Discussion 2
   1.1.1. General Background 2
   1.1.2. Specific Problems 3
   1.2. Purpose of Thesis 4
   1.3. Structure 4
2. Theory 6
   2.1. Triple Entry Accounting 6
   2.1.1. Accounting History 6
   2.1.2. Principles of Triple Entry Accounting 7
   2.2. Blockchain 9
   2.3. Blockchain Structure 12
   2.3.1. Consensus 15
   2.4. Smart Contracts 17
3. Previous Studies and Literature 19
   3.1. Accounting on the Blockchain 19
   3.2. Auditing 22
   3.3. Smart Contracts 24
   3.3.1. Automatic Real Time Accounting 25
   3.4. Limitations and Drawbacks 26
4. Methodology 30
   4.1. Qualitative 30
   4.2. Hypothesis 31
   4.3. Data and Sources 32
   4.4. Interviews 33
   4.4.2. Interview Guide 35
   4.5. Conducting Interviews 36
   4.6. Data Saturation and Analysis 37
5. Discussion on Findings 39
   5.1. Interview Questions and Answers 40
   5.2. Analysis of Questions 41
6. Conclusions 53
   6.1. Limitations 55
   6.2. Future Studies 56
7. Summary in Swedish 57
   7.1. Inledning 57

7.2. Syfte 57
7.3. Teori 57
7.4. Tidigare Studier 58
7.5. Metodologi 60
7.6. Analys av Frågorna 61
7.7. Slutsatser 64
Word List 67
References 69

ÅBO AKADEMI UNIVERSITY – Faculty of Social Sciences, Business and Economics

Abstract for master's thesis

Subject: Accounting
Writer: Niclas Gröndahl
Title: Accounting, Auditing and Blockchain - Interviews with Finnish auditors about blockchain
Supervisor: Ralf Östermark

Abstract:

Blockchain technology is something that is often mentioned in the same context as bitcoin. The technology in question has, by some, been touted as the fourth industrial revolution, which will change how we conduct business.

There exists a lot of academic articles on what benefits blockchain could provide for accounting and auditing, but very few studies that have been conducted with asking what the auditors themselves think of the technology. This is the first study of its kind in Finland, and with Finns tending to be early adopters of technology, consulting professionals in Finland can be considered a good idea.

This thesis serves as an analysis on blockchain knowledge among auditors in Finland. The auditors that partook in the interview were divided into three groups, which had different amounts of work experience. This allows for the study to get a good range of opinions on the technology, from both new auditors and experienced auditors.

The results of this thesis show, that the auditors in Finland were aware of blockchain technology, but most were not exactly aware of in what way it can help. When further explored, the majority did think it could provide some benefits, especially when it comes to smart contracts. However, the main principles of immutability did not completely convince the auditors, as the information entered could be manipulated before it reached the blockchain.

Keywords: Accounting, Auditing, Blockchain, Triple entry accounting, Smart Contracts

Date: 17.5.2020 | Number of pages: 84

1. Introduction

Although much of the interest around blockchain the previous years has been focused on bitcoin and other cryptocurrencies, their skyrocketing prices and subsequent downfall in value, there is an inherent value in the underlying technology of blockchain. According to industry leaders, blockchain, which is a decentralized digital ledger, could be considered the fourth industrial revolution. It is an entirely new way of performing business and related functions, such as accounting and auditing.

While double entry accounting has proven to be versatile and has been credited in allowing companies to grow, prosper and spread around the world, it does have drawbacks which are not often discussed, with one of these being security (Carlin, 2018). We have managed to computerize accounting well, but it is only a computerized version of double-entry accounting and has not evolved to take advantage of computers. Just as double entry accounting on paper, computerized systems are open to fraud and potential abuse (Carlin, 2018). The suggested triple entry accounting that blockchain provides could potentially minimize these issues through providing a third entry, a cryptographic signature of the transaction (Grigg, 2005). Each and every transaction now has a unique and immutable identifier, which can be traced back to its point of origin and who authorized it (Grigg, 2005).

With people believing that blockchain is the fourth industrial revolution, major changes in a multitude of industries are expected. For example, supply-chain records would be immune to tampering, and records would always show the true point of origin (IBM, 2018a). Accelerating cross-border transactions and remittances is currently under way, with Alibaba Cloud and other financial services showing interest in using blockchain technology for this expressed purpose (Alibaba Cloud, 2018; Santander Bank, 2018). Banks are also exploring the possibilities of blockchain, Nordea and other banks have launched WeTrade, which is a finance trading platform, which works on blockchain technology provided by IBM, called Hyperledger (IBM, 2018b). In the medical industry, companies are exploring the possibility of encrypting patient records, sealing them and keeping them safe in a tamperproof environment, in addition to being able to have all the changes traceable (Deloitte, 2018).

There is active development and research into how blockchain could be utilized. Among those who have been researching the potential of blockchain technology are the Big 5 accounting companies (i.e. Deloitte, EY, KPMG, BDO and PwC). As an example, both KPMG and Deloitte have been researching how blockchain could help accountants and auditors create a more secure and efficient accounting/auditing environment (Deloitte, 2016; KPMG, 2018a).

PwC France is currently working together with a blockchain start-up called “Request Network”, who are developing a blockchain accounting solution (PwC, 2018). Factom is another company working on how to implement audit trails on the blockchain (Deery, Lu, Johnston, & Kirby, 2018). One of the significant developers working on accounting on the blockchain is the Ethereum based “Consensys” foundation, which is developing an accounting suite called “Balanc3” which operates on the Ethereum blockchain network (Balanc3, 2017). Other organizations have sprung up to further the development and adoption of accounting on the blockchain, the largest one currently is called the “Accounting Blockchain Coalition”, which has representatives from the Big 5 accounting companies (ABC). SWIFT, which is the de-facto standard in secure transmission between financial institutions, is working together with R3 to improve speed and security (CNBC, 2019).

Whether blockchain is the future of accounting is still uncertain but considering many famous institutions that are active in accounting and auditing have expressed interest in blockchain, it is important for academics of accounting to view the potential disruptions and changes it could bring.

A word list has been provided on page 67 that explains key terms used throughout this thesis.

1.1. Problem Discussion

1.1.1. General Background

Yet, there is a need for some extensive studies on whether accounting or auditing on the blockchain is worth pursuing, or if it is something auditors and accountants here in Finland are interested in. The Big 5 accounting companies abroad have publicly expressed interest in the application of blockchain in both accounting and auditing, but little academic research has been conducted. The belief of some of the Big 5 is that blockchain would make accounting much more streamlined, as well as helping

auditors decrease their workloads and automate many of the simple processes that take up a lot of time (Deloitte, 2016). All Big 5 accounting firms have their own blockchain labs where they are experimenting with the technology, and some have already released working products based on blockchain (KPMG, 2016). However, the single most important factor for all the Big 5 accounting companies seems to be the transparency that blockchains could potentially offer.

1.1.2. Specific Problems

As mentioned in the introduction, many of the fraud scandals in accounting have been caused by shortcomings and flaws in the double-entry bookkeeping, and the lack of transparency (Grigg, 2005). Accounting has been similar for almost 700 years at this point, and technology has been advancing rapidly, but accounting has remained the same, only the medium it is conducted on has changed from paper to the computer. It has been suggested that blockchain could potentially decrease the fraud risk by being a trustless network. On average fraud loss is USD 2.75 million dollars, according to the Association for Certified Fraud Examiners (2019), in their 2018 report. The most common one being asset misappropriation and the most devastating one being financial statement manipulation (ACFE, 2019). In other words, there is a need for a more fraud proof system, and blockchain might solve that problem.

EY has the belief that blockchain will have the same impact as enterprise resource planning systems (ERP) have had on the world (EY, 2017). Blockchain would increase transparency in the organization and potentially eliminate many of the intermediaries. This in turn would help reduce fraud through “enhanced identity management” as EY calls it (EY, 2018a). KPMG also believes that blockchain could be used to help reduce fraud at companies, due to its immutable and transparent structure (KPMG, 2018b). Any strange transactions would have an easy audit trail to follow (KPMG, 2018b).

Considering the benefits that blockchains could provide, the opinions of auditors are important to hear.

1.2. Purpose of Thesis

The purpose of this thesis is to measure the receptibility of accountants and auditors in Finland on whether the Finnish market is interested and aware of accounting and auditing on the blockchain. Since auditors are experts in both these areas, their opinions are important for any future developments in these fields.

There has not been almost any public discussion on accounting and auditing on blockchain in Finland, this study will try to remedy that situation. No studies of this kind have so far been made in Finland and in general this is one of the very few studies that have been conducted on what auditors themselves think of blockchain. As the technology is new, the assumption is that only few know about it, but the questions that will be asked might provoke thoughts about the future of accounting and auditing.

1.3. Structure

The structure of the thesis is as follows: It will open with an introduction where the basic premise of triple entry accounting is explained, and how it can help solve some of the shortcomings that have been linked to double entry accounting. After this the purpose of the thesis is explained and the structure for the thesis is laid out. The second chapter serves as an explanation on what triple entry accounting is, what blockchain is, how it works and what forms of blockchains exist. The chapter is meant to serve as a primer for those who are not aware of how blockchain technology works.

The third chapter is a literature review on blockchain and accounting, as well as auditing and smart contracts. The last part of the chapter is dedicated to explaining some of the drawbacks and disadvantages of blockchains when coupled with accounting and auditing functions.

The fourth chapter is dedicated to the methodology of the thesis, where the research method is explained and the questions that will be used are presented. In this chapter the hypothesis for the thesis will also be presented which questions are going to be asked.

The fifth chapter will be used to present the findings of the interviews that were conducted. The purpose of the questions will be explained, and why these questions are relevant for this study.

The sixth chapter will serve as a conclusion for the thesis where the results will be discussed and ending remarks will be made. In this chapter future research will also be potentially suggested.

2. Theory

This chapter focuses on explaining the basics of some of the fundamentals of blockchain, as well as explaining why some believe that blockchain would be conducive in transforming accounting to a more fraud-proof format. The goal of this chapter is to build a foundation for people who are not knowledgeable on what blockchain (and distributed ledger technology) is and explain the basic concepts. Additionally, the reader will also get a brief explanation and introduction to what smart contracts are. At the end of this chapter, the reader should have a basic understanding on blockchain and smart contracts.

2.1. Triple Entry Accounting

2.1.1. Accounting History

The concept of triple entry accounting was first introduced by Ian Grigg (2005), and is not to be confused with another concept called momentum accounting which is also sometimes referred to as triple entry accounting. Triple entry accounting in the context of Ian Grigg, is accounting with three entries, one extra in the addition to the traditional two (Grigg, 2005). However, before discussing more about triple entry accounting, it is worth looking at the history of accounting, and how it has evolved to what it is today.

Single-entry accounting was invented around 5000 years ago in Babylon. This is the simplest and most basic form of accounting that exists (Alrawi & Ambashe, 2018; Cîndea, Cîndea, Ciurariu, Trifu, & Durdureanu, 2011). In single-entry accounting one creates a list of assets or debts, and when an asset is bought or a debt is incurred, it is added to the list, and when the asset is sold, or the debt is paid, it is removed from the list (Grigg, 2005). The single-entry system works well for the most basic needs; however, it is not sustainable for anything but the most basic lists. One of the issues with single entry, is that mistakes can easily occur without noticing them much later, as well as it being easy to manipulate. The reason for single-entry accounting being easy to both manipulate and why it is prone to errors is in its construction, it is a simple list. If liabilities and assets are being recorded on a simple list, there is no true verification that your assets and liabilities are in balance (Grigg, 2005). When one is unsure whether the error is simply an error or, if it is a case of fraud, the situation can

become quite severe. Single-entry accounting was used for around 4400 years, until the invention of double-entry accounting.

Double-entry accounting is said to have been invented in the 15th century by a Venetian friar by the name of Luca Pacioli (Cîndea et al., 2011). It is often speculated that the invention of double-entry accounting is what allowed the Venetian merchants to flourish in wealth and trading, as well as dominate in trading around the world. Eventually, double-entry accounting spread to the rest of the world and became the predominate and only way of conducting accounting (Cîndea et al., 2011).

Simply put, in double entry accounting a transaction generates both a debit and credit event. As an example, when someone purchases inventory or products there is a debit transaction in the inventory and a credit transaction in the bank account. The obvious benefit of double-entry accounting is that every transaction creates two events that cancel out each other. This in turn translates onto the balance sheet, where we can see whether our accounting balances. When credit and debit eliminate each other, the balance sheet will balance itself out. However, if for some reason there no longer is a balance, the error can be located quicker and easier, when compared to single entry accounting. In general errors are easier to find, and manipulation as well as fraud is harder to execute (Carlin, 2018).

However, as great as double-entry accounting is, it still has flaws. Many of the accounting scandals in the past decades have been caused indirectly and directly by some of the inadequacies and shortfalls of double-entry accounting. Most of these are related to fabricated verifications and transactions, which allows fraudulent transactions to slip through the internal controls (Grigg, 2005). These inadequacies are often mitigated through audits that are conducted on a regular basis. These, however, are also prone to error, but it is better to have a control measure to try and prevent mistakes from occurring. Audits have not prevented large scale frauds from happening either.

2.1.2. Principles of Triple Entry Accounting

Triple-entry accounting expands the principle of double-entry accounting, by adding a third entry, “the receipt”. According to Ian Grigg (2005), transferring double entry accounting from paper to computers has not been as efficient as desired.

Computerized accounting systems still rely on double-entry accounting that was meant to be done in paper form. Ian Grigg (2005) argues that we are not taking full advantage of accounting on computers since the power given by computers is not leveraged. Instead of trying to adapt double-accounting entry for computers, we should focus on creating a new form of accounting that is meant for computer use and will use computer science to make it more secure and efficient.

Triple-entry accounting, as its name suggests, has three entries: debit, credit and the receipt. These three entries are divided among three different parties, the payer, issuer and payee. The payer is the person initiating the payment, the issuer is the verifier and signer of the payment, and the payee is the person receiving the payment (Grigg, 2005). A theoretical scenario where person A is going to pay person B, explains the potential system well: When person A pays person B, it passes through an intermediary called C. The intermediary C confirms that the payment has been received by B and produces a receipt of the transaction and sends it to both parties. (Grigg, 2005)

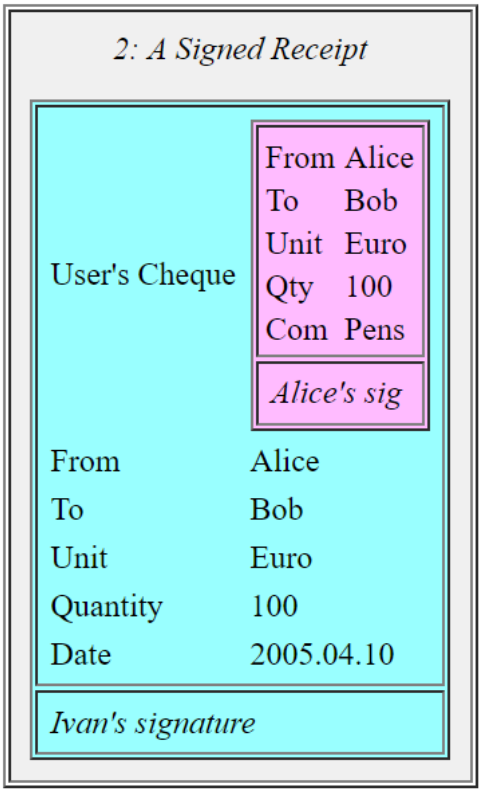

Figure 1 Example of what the third entry could look like. Grigg 2005

The receipt includes the entire transaction, from both the perspective of the sender and recipient, as well as the so called “digital signature” of who both parties. The digital signature, as Grigg (2005) explains, can be seen as signing a cheque or signing a document with a personal cryptographic key. In today’s world, the receipt is the dominating proof that a transaction has occurred, for example going to the store and purchasing an item and you get a receipt for your purchase. Not only does the receipt work as evidence that you bought an item, but it also safeguards the shop owners from potential fraud by employees.

One of the largest drawbacks of Grigg’s model (2005) is the requirement of a neutral, trusted or an independent third-party who is assigned to verify the transactions, and in the previous example that would be C. A human element as a third-party verifier makes it vulnerable to exploitation and therefore should not be pursued. A third-party verifier themselves could become corrupted and act in their own self-interest, be a target of cyberattacks and more.

However, since the time of writing his article in 2005, technology that could make it feasible to have a trusted third-party acting as a verifier, has come a long way. A technology named blockchain was introduced in 2008, and it might change how we interact with

2.2. Blockchain

The concept of blockchain technology comes from a whitepaper written by a person or group using the pseudonym “Satoshi Nakamoto”. This whitepaper was called “Bitcoin: a peer-to-peer electronic cash system” and was the presentation of a decentralized computer protocol by the name of “Bitcoin”. The primary purpose for the creation of bitcoin, was to offer another alternative to the traditional financial system and circumvent the third parties that work as a middle hand for transactions, through creating a “trustless” financial system. Nakamoto (2008) explains the problem with the current financial system as follows

> “The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than

> they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party."

A trustless financial system is self-explanatory; it is a financial system that works without trust, and for bitcoin to be able to work on a trustless level, an underlying technology was created, the "blockchain" (Nakamoto, 2008).

Blockchain technology is a digital ledger that is decentralized, a centralized blockchain would be a normal database. A blockchain is a collection of records, same as a ledger, but spread across a distributed network of computers, which are called nodes (Kokina, Mancha, & Pachamanova, 2017). Every computer on the distributed network has the exact same information as any other, and they all work together to verify that the information on the network is correct. Once a transaction on the blockchain has been approved and recorded, it can no longer be altered, the information becomes immutable. In the case of bitcoin, it uses the processing power of computers to verify the transaction, in something called "mining".

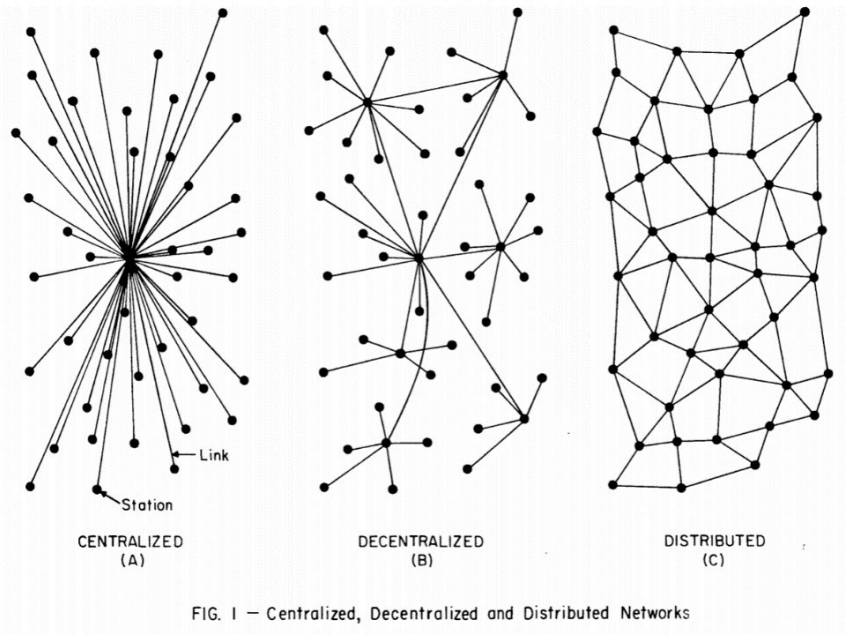

Figure 2 Illustration of networks (Baran, 1964)

Mining is the creation and verification of the blocks in the blockchain, which are the entries in the blockchain that can be seen by the entire distributed network. Before a block is added and approved to the network, the information in the block is validated

by the nodes, and when they reach “consensus” it is appended to the blockchain in a chronological order to establish a continuous record (Kokina et al., 2017; Zheng, Xie, Dai, Chen, & Wang, 2018). Information in a block can theoretically be anything; transaction information, products, health records and more (Kokina et al., 2017).

The name blockchain comes from the structure of the records. Every block has information that ties back to the previous block, which allows it to become a chain of immutable ledger of transactions (Kokina et al., 2017; Zheng et al., 2018). If the distributed network detects an error in the information, it will not validate the block, and it will not be added to blockchain. The real nature of the decentralization allows it to work without trust, since there is no central authority, but instead the miners and their nodes on the network all work together to verify the authenticity of the transactions.

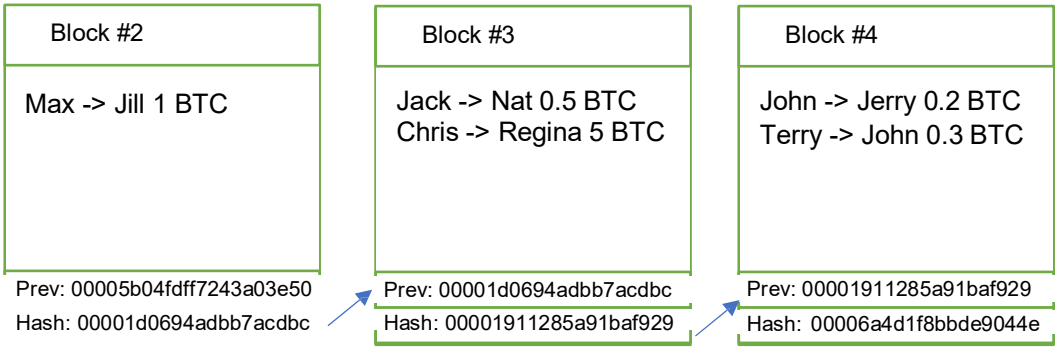

Figure 3 Example of transactions on a blockchain

In the above example, we can see a simplified example on how blocks on a blockchain functions like, and what information it can contain. The blocks are each linked to the previous block, and in the blocks, we can see the transactions that were confirmed and verified to have happened during that verification time limit. The information that has been stored on the blockchain is immutable and unalterable, unless a successful attack is launched against it (Zheng et al., 2018). These attacks will be explained in a later chapter.

The creation of a block requires the solving of a cryptographic puzzle, which means the solving of a “nonce”. The efficiency of the network is measured in “hashing power”, which comes from the amount of power the entire distributed network is using to solve the puzzles and create new blocks (Kokina et al., 2017).

Incentivizing people to participate in the creation of blocks is important, and that is where mining comes in. In the case of the “Proof-of-work” consensus mechanism, miners who create the new blocks must lend their computers to mine the new blocks (usually through using their GPUs or CPUs, but other methods exist as well) (Gabison,). By participating in the creation/discovery/verification of the block they receive a reward. When mining Bitcoin for example, when a block is found by miners, all those who participated in mining the block are rewarded with bitcoin. Those who lend more computer power to mining the network, are rewarded with more bitcoin. Mining also works as a form of spam protection, since mining costs resources (time and power), people who want to use the network maliciously or attack it, need to invest in capabilities to overpower all the other users on the network.

This is where triple-entry accounting meets the blockchain. One of the shortcomings of the suggestion by Griggs (2005), was that a third party should be in control of approving transactions. However, this is a potential point of failure, as there is no guarantee that a person will not be influenced or that they are secure against cyberattacks (Grigg, 2005). The blockchain solves the third-party issue, since in theory it should be completely decentralized and distributed. No single person can have control over the network and make it go against the will of the other nodes, as the consensus mechanism will prevent this from happening. But this brings us to another question, whether the blockchain should be open to everyone or open only to those that have been verified by a central authority, in other words what the different structures of blockchains are.

2.3. Blockchain Structure

A permissioned blockchain is a blockchain where users are selected by a central authority on whether they should be allowed to participate on the network. This is theorized to be how organizations will want to have their blockchains used, as they then may control who can participate on the network (Feng, He, Zeadally, Khan, & Kumar, 2018). This in turn means that they can keep the network secure and private from outsiders (Dai & Vasarhelyi, 2017). However, this can lead to situations where someone gains access through a permissioned users’ credentials to the internal network, and hence they might execute attacks that can render the information on

the blockchain unusable or copy the information on the blockchain. Permissioned blockchains usually have less users than permissionless blockchains and this fact might expose the blockchain to these kinds of situations.

These permissioned blockchains are also sometimes known as consortium blockchains, one example is IBM's Hyperledger (Zheng et al., 2018). Consortium blockchains are specifically aimed at organizations that want to use blockchain, but which do not want to develop their own blockchain solution in-house, and instead opt to use a pre-existing network.

A permissionless, or public blockchain is for example, Bitcoin or Ethereum, where anyone that wants to participate, can participate (Feng et al., 2018). This allows for large networks to be created, where there is a much larger certainty that no single entity has control of the entire network. This does come with some drawbacks though, namely privacy and speed. If a blockchain is permissionless, it is open for everyone to use and therefore all information on the blockchain can be seen by everyone (Feng et al., 2018). Although we can see only hashes of sending and receiving addresses (called pseudonyms), it does not mean it is impossible to figure out who is behind the pseudonym (Feng et al., 2018). In contrast to bank accounts where transactions are seen by only parties that are interacting with each other, all transactions on the permissionless blockchain are visible to everyone (Feng et al., 2018).

Another issue is speed, which often referred to as "scalability" (Dai & Vasarhelyi, 2017). The current speed of the Bitcoin network is seven transactions per second (tps), and for a small company this should not be an issue. However, scaled up to a large corporation or a globally spanning one, speed will become an issue. Permissionless and highly decentralized blockchain networks often have a lower tps. When the blockchain is centralized the speed increases (Dai & Vasarhelyi, 2017). The problem is that this goes against the decentralization that blockchains provide, and instead becomes a centralized database. There are some consensus forms that allow for a more centralized approach, but keeping it decentralized to certain degree. These consensus mechanisms will be presented closer in chapter 2.3.1.

The final form of blockchain is the private blockchain, where the entire network is under the control of one entity (Zheng et al., 2018). This is where one could start questioning whether it is in fact anymore a blockchain or a centralized database. The private blockchain could have a very fast tps rate but is most at risk for insider attacks.

Different blockchains serve different purposes and function in different ways. For example, Bitcoin and its blockchain are meant to be used a currency, while Ethereum, the third largest cryptocurrency, works as fuel for the its blockchain network. Ethereum also includes tokens, which fuel decentralized applications (Zheng et al., 2018). To be able to participate, to send or receive a currency or a token on a blockchain, a "wallet" is needed. One could think of the wallet as bank account, or digital wallet. In this wallet you store your currencies and tokens. There are two key items to using a blockchain wallet, the "public key" and the "private key"(Zheng et al., 2018). The public key is the address cryptocurrencies are being sent to, which can be compared to IBAN or any other similar bank account identification number. The private key is a cryptographic key that is used to access your wallet and allows you to execute actions (Zheng et al., 2018). If you would want to move funds from wallet "A" to "B", you would first need to know the public key of wallet B (Zheng et al., 2018). After you have received the public key for the wallet you are sending cryptocurrencies to, you must now enter your private key linked to the wallet you are using to send the cryptocurrency. By entering your private key into wallet "A", you have now authorized and signed the transaction.

Figure 4 Example of Public Address on Bitcoin

The private key is akin to the digital signature Ian Grigg mentioned in his paper on triple entry accounting (Grigg, 2005). By entering a personal private key, the transaction is signed and approved by the blockchain. Every private key is a unique cryptographic key that is used to approve transactions on the network (Zheng et al., 2018). The blockchain confirms the transaction is correct and authorizes it. It is important to be aware, that private keys are meant to be private, and not shared. If a private key ends up in the wrong hands, losing all funds is a real and dangerous possibility.

2.3.1. Consensus

As mentioned in the previous chapter, there exists multiple ways of forming consensus on a blockchain network. Among these are proof-of-work, proof-of-stake, proof-of-burning, and many more (Gramoli, 2017). The purpose of these consensus mechanisms is to reach a consensus by all participants on what should be done with each block. This is what gives the blockchain its trustless form, no centralized entity is deciding on what should be done next. Therefore, it is important that the most common ones are explained, to give a better understanding what some of the benefits and drawbacks, and which companies interested in blockchain uses might be looking at.

Proof-of-work (PoW) is the most famous example, which was created for Bitcoin (Kokina et al., 2017). A large decentralized computer network with nodes is tasked with mining blocks to further the blockchain by offering their power to solve cryptographic puzzles. Miners are the people who lend their GPUs or CPUs to conduct the verification of the blocks, and they are rewarded by the amount of hashing power they input to the network.

There are drawbacks with a consensus mechanism like proof-of-work. One of these is the required amount of power to run a blockchain network with this consensus mechanism (Kokina et al., 2017). As the number of participants on the network increases, there is more hardware solving cryptographic calculations, which in turn means that the difficulty of the calculations increases. As the hardware required to solve the calculations becomes more advanced, the required power to operate the blockchain increases, which can lead to a strain on the environment. In other words, from an environmental perspective, proof-of-work is not the best option (Truby, 2018). Another issue that is related to this form of consensus mechanism is the so called 51-percent attack (alternatively called majority hashrate attack) (Gramoli, 2017). The name of the attack implies that a party or an entity manages to capture 51 percent of the entire networks hashing power and is now the majority owner of the entire network. One of the practical benefits of a proof-of-work network, is that an attack like the 51-percent attack requires a considerable amount of power, which translates into a significant expenses for the attacker (Lai & LEE Kuo Chuen, 2018). A 51-percent attack is a rare occurrence, especially on a public network, due to the amount of computing power that is required to gain most of the hashing rate.

However, if someone did manage to successfully execute a 51-percent attack, the blockchain would be compromised and information should not be trusted before an independent analysis could confirm the status of the information on the blockchain.

A 51-percent attack allows one to overcome the mutability of the blockchain by allowing alterations of the previous blocks. This is a resource intensive task, as it requires one to recalculate the previous blocks. If the information one wants to alter is in block 20, and the current block is 200, it would mean they have to recalculate 180 blocks to be able to alter the information.

Proof-of-stake (hereafter PoS) is another form of consensus mechanism and works entirely differently to proof-of-work. Instead of using computer's CPU or GPU to solve cryptographic puzzles, the number of tokens you hold grants you more power over the network. By using PoS, there is hope that the costs of running a blockchain would dramatically decrease. A PoS blockchain does not require GPUs or CPUs to mine blocks but are instead validated by nodes that hold a certain amount. This is the reason they are named "forgers" instead of miners since they forge a block into existence. In general, the amount of currency or token that one holds on the PoS blockchain, gives one more control over the network. This in turn means that you also receive more rewards for the forging that is done. In the case of a PoS blockchains, the reward constitutes of the transaction fees from the transactions made on the network during the forging period. Ethereum is currently a PoW blockchain but is planning on moving to a PoS system in the future. The danger of the PoS consensus method is that, since the cost of mining/forging is near to zero, attacks on the network would become easier to perform. False "stake" attacks are a possibility, which means that the attacker fakes the size of their stake. Other coins and blockchains have suggested other ways of mitigating the danger of attacks through proof-of-activity, where a certain number of miners need to sign and verify the creation of the block. This would prevent a total control of the network, as they could not singlehandedly create the blocks, even if they would own 50% of the entire stake of the network (Zheng et al., 2018).

Delegated proof-of-stake (hereafter DPoS) is a variation of proof-of-stake but is more centralized. Instead of allowing anyone to participate in the network, only people voted in (or selected) can vote/participate in the creation of blocks (Zheng et al.,

2018). One of the big contentions with DPoS is the centralization of nodes, potential collusion and vote buying. Blockchains that utilize DPoS usually have better tps rate, as there is less decentralization (Zheng et al., 2018).

Practical byzantine fault tolerance (hereafter PBFT) requires that all the participants of the network are known. This is the consensus mechanism that Hyperledger, IBM's consortium blockchain, uses (Linux Foundation, 2018). In the PBFT it is assumed that the number of nodes that are malicious do not exceed 1/3 of all nodes (Zheng et al., 2018). The more nodes are on the network, the less the chance of malicious nodes taking over the network. However, it is still prone to sybil attacks (also known as 51-percent attacks), where a party can gain or create several identities and gain majority of the network.

Proof-of-burn is a consensus method where a small number of tokens is discarded after every transaction, as a mechanism to verify that a transaction truly has occurred. This is one of the most environmentally friendly forms of consensus mechanism, as it does not require you to own the cryptocurrency. Instead, whenever a transaction happens, a small number of tokens or cryptocurrencies are sent to a discard address, often called "burned tokens". By sending these burnt tokens to the discard address, it verifies that the transaction indeed has indeed occurred.

2.4. Smart Contracts

For many people smart contracts are one of the most interesting features on the blockchain. Smart contracts are not "smart" or independently thinking contracts, but pre-programmed computer programs that fulfill an action when pre-determined conditions are met. These contracts were first mentioned by Nick Szabo (1994). The idea of a smart contract is to automate simple and repetitive tasks or to have them monitor certain conditions and then execute when the condition has been met. There is an ongoing debate whether these computer programs in fact should be called "smart contracts", but no consensus has yet been reached.

Smart contracts are not a foundational part of the blockchain structure but more an addition. Initially bitcoin had a very rudimentary and simple smart contract system, and smart contracts were more properly integrated after Ethereum was introduced by Vitalik Buterin (2013). According to Buterin (2013), smart contracts are:

> “systems which automatically move digital assets according to arbitrary pre-specified rules.”

Buterin (2013) also mentions that smart contracts can run autonomous organizations, also known as DAO’s (Decentralized Autonomous Organization). These organizations are autonomous organizations that are completely run and built on smart contracts and need minimal human interaction to function.

The largest strength of smart contracts is the ability to be cost-efficient, by removing intermediaries. By getting rid of intermediaries, such as banks and credit providers and the like, the process of transactions is speeded up by having it autonomously execute them (Rozario & Vasarhelyi, 2018).

Smart contracts come in several sizes and shapes. For example a smart contract can be a simple program for paying the rent for an apartment, or there could be a smart contract that hedges oil prices or monitors the stock market and sells stocks at a certain price (Rozario & Vasarhelyi, 2018). After the introduction of smart contracts on Ethereum, many other platforms have been created to compete with Ethereum. All the blockchains operate in different ways and solving different problems.

As the functions of blockchains have been explained, it is worth looking at how these can be applied to accounting and auditing. This will be expanded upon in chapter 3, previous studies and literature.

3. Previous Studies and Literature

This chapter focuses on studies made on blockchain and their impact on both accounting and auditing. Blockchain is fairly new technology, which in turn means there has not been much previous research conducted in this area. Most studies focus on auditing and how their job descriptions will change. One of the reasons for this could be that the changes to accounting are more technically oriented. The chapter also looks at how smart contracts are a part of the blockchain ecosystem and how they might impact accounting and auditing. This chapter will also look at studies that explore the potential downsides of using blockchain in an accounting and auditing environment.

3.1. Accounting on the Blockchain

As previously discussed, the basic principle of accounting the blockchain is triple entry accounting. In triple entry accounting we have three different entries: credit, debit and the third entry, the receipt. Instead of using a neutral third party as required in Griggs (2005) suggestion, the blockchain is used. The largest issue with using a neutral third party are the guarantee that the third party will stay neutral, that information is not lost, nor that the data are potential targets of cyberattacks (Grigg, 2005). When a transaction occurs on the blockchain, a receipt is created. This is stored on the blockchain and all parties involved in the transaction can see it (and if it is a public blockchain everyone can see it).

Deloitte (2016) explained in a research study how blockchain accounting could potentially change the way we perceive accounting. They state that instead of having separate registers for all records (invoices, receipts and more), everything can be written into blockchain transactions which would work as a joint register and would thus become “an interlocking system of enduring accounting records” (Deloitte, 2016). These records are then, as previously mentioned, cryptographically sealed (or encrypted), which means that any form of tampering would be noticed and would leave a trace. Another Big 5 company, EY, has stated that the use of blockchain would make transactions easy to follow, from point of origin to end (EY, 2016). Both Deloitte and EY emphasize that by using blockchain, all transactions have a shared ledger, where confirming accuracy is made simpler. Another benefit with a shared

ledger is through reconciliation, which according to EY, makes companies lose “50 and 100 working days” in reconciling differences (EY, 2016).

Dai and Vasarhelyi (2017) have an example of what a potential blockchain accounting solution could be like. Every debit and credit transaction within an organization would create a blockchain entry, which is included in the traditional double-entry accounting system. Transactions in the blockchain are recorded as token transfers between the different blockchain accounts.

In this case, a token is a so-called tokenization of an asset or value (Dai & Vasarhelyi, 2017). Instead of being a real asset that is booked on the blockchain, it is a representation of the asset. For example, the transactions we mentioned before are only token transfers between the blockchain wallets, and in this token is the information of the transaction that occurred between the real-world accounts, what the asset actually was and the reason for the transfer. Tokenized assets can be almost anything; securities, commodities, gold, buildings and so forth (EY, 2018b). These are sometimes called “colored coins”.

Perhaps the largest benefit of accounting on the blockchain would be immutability, which in its turn can be a drawback. Once information has been entered onto the blockchain, the information cannot be altered, and this can be verified by looking at the hashes (Dai & Vasarhelyi, 2017). If the hashes on the blockchain entries are different from before, information has been altered. However, if wrong information is entered onto the blockchain, changing it becomes more difficult as it is “appended” only.

Prevention or deterrence of fraud would also be efficient due to the design of the blockchain. If someone wants to alter or remove accounting records, he would have to know which block contains the information he wants, that is pertinent to his cause, and after this you need to recalculate and verify this block (Appelbaum & Nehmer, 2017). In itself this is already computationally expensive, since it requires majority control over the network, but as an example: if the block that they want to change is block number 357, and the current block is number 438, they would need to recompute every hash between block 357 and block 438, and if any new blocks are appended to the chain, they will have to calculate those as well, increasing the workload for the attacker (Appelbaum & Nehmer, 2017).

The American Institute of Certified Public Accountants (AICPA) and Chartered Professional Accountants of Canada are also looking into the development of blockchain and educating their members on the basics of what a blockchain is and how it might affect accounting and auditing (AICPA, 2017).

Other suggestions have been to incorporate blockchain into ERP systems that would give companies an easy way to conduct accounting on the blockchain (Dai & Vasarhelyi, 2017). By incorporating a blockchain solution into how an already existing ERP system would make it easier to transition from an organization-wide perspective (Dai & Vasarhelyi, 2017). In a scenario like this, the entire system would not have to be replaced, only the accounting infrastructure would be upgraded. This of course does not mean they could avoid large scale investments, as it very much depends on the architecture of the blockchain they have decided to use. A way to avoid or mitigate infrastructure upgrade costs, is by using a cloud ERP, that would potentially offer lower costs for organizations that want to engage in blockchain accounting (Dai & Vasarhelyi, 2017).

Yu, Lin & Ting (2018) offer one of the more comprehensive papers that look at how financial accounting would work under a new system like the blockchain, in both the short and long run. In their paper, they come to a number of different conclusions. In the short run, blockchain will be hampered with technical limitations, such as scalability, because big firms generate a massive amount of information in a short span of time and blockchain could have issues keeping up (Yu et al., 2018). They also posit that accounting information would be available for anyone to download and watch, which could scare away potential users. Add to this that the costs of implementing a blockchain accounting solution might be expensive, as they might have to potentially overhaul their entire accounting system (Yu et al., 2018). However, there are still benefits in the short run, among them that blockchain is a good solution for voluntary financial disclosure, to reduce information asymmetry with their shareholders and investors (Yu et al., 2018). In the long run, the authors believe that blockchain will have a very positive impact on financial accounting, as it could reduce errors in disclosures, increase quality and even more mitigate the information asymmetry (Yu et al., 2018). However, even with this change, people can still abuse the system.

Although the five big accountancy firms are currently researching accounting implementations on the blockchain, there have been very few academic studies into the drawbacks and benefits of accounting on the blockchain (Carlin, 2018). There are several suggestions on what it could entail, but these studies have not translated into any physical implementations or case studies. However, there have been significantly more studies into the auditing side of blockchain, which is what the next chapter is about.

3.2. Auditing

Although accounting might be in turn for a paradigm shift, the auditing profession might be even more challenged. There have been several exploratory studies into how blockchain could potentially change the auditing profession, or whether auditors are still needed to the same extent as before.

Rozario and Vasarhelyi (2018) discuss in their paper “Auditing with Smart Contracts”, that blockchain could change the nature of auditing. The smart contracts on the blockchain could potentially increase the audit quality and as well give the information stakeholders want and require for making decisions. Auditors will need to keep up with the technological advancements that are currently going on and be proactive in helping shape the future of their profession (Deloitte, 2016). Some of the Big 5 are already offering courses and education for their employees in blockchain technology.

Kozlowski (2018) writes in his paper how auditing needs to adapt to the information age, there needs to be a new framework that can be used for the blockchain. First, it needs to be adaptive, where auditors are to put more focus on learning to understand the smart controls and contracts and be able to read them and analyze what the smart contracts are doing. They would be performing fraud detection, risk assessment and systemic evaluations, a step up from record tracing and verification (Kozlowski, 2018). Second, it needs to be scalable due to the different sizes of blockchains and storage options, as well as potential use of big data at their clients. Third, a distributed approach is needed, where auditors will be able to make decisions and act independently in a local setting, without having to interact directly with the client.

A caveat to triple-entry auditing is that all accounting must be performed on the blockchain (Simoyama, Grigg, Bueno, & Oliveira, 2017). By having all the records on the blockchain, it theoretically should be easier and faster for auditors to pull information directly from the blockchains of the company, being audited (Dai & Vasarhelyi, 2017). Records would not have to be pulled out of physical storage, and instead auditors would look up what they need and want to investigate through queries (Dai & Vasarhelyi, 2017). Deloitte (2016) writes in their report, that blockchain offers a great chance of making the job of auditors more efficient and speedy. Instead of having to ask the company being audited to manually retrieve documents, all information would be more accessible straight from the blockchain, and time-consuming audit preparation work would be decreased for management (Yu et al., 2018). Some authors have suggested this will change how auditors conduct their work, where instead of focusing on testing samples they can now focus more on verifying that internal controls are effective (Yu et al., 2018).

As information is stored on the blockchain, meaning a decrease in audit preparation, near real-time audit work could be possible for routine items and freeing the auditor to focus on more complex transactions (Deloitte, 2016). They also posit that with the digitalization of their work, the auditor's workload could be automated, together with machine learning and analytics and suspicious transactions could be reported in real-time (Deloitte, 2016). If support documents could be uploaded and encrypted and linked to a blockchain and its entries, it could speed up the speed of financial reporting and auditing (Deloitte, 2016).

The future auditor might need to be able to read and understand code to be able to audit smart contracts, or perhaps this will give room for an entirely new branch in auditing (Deloitte, 2016). According to Deloitte, CPAs will provide assurance to the users of the technology, thanks to their independence, objectivity and expertise (Deloitte, 2016). As previously mentioned, auditors might have to become more versed in different coding languages to provide assurance services to interested parties. Auditors might also work as oracle auditors, who evaluate the connections of the blockchain and smart contracts, outside of the company. Looking for vulnerabilities, errors and malicious intent would be the most important part of these auditors (Deloitte, 2016). In the future, auditors might even work as "service auditors" for consortium blockchains, where they verify applications and smart contracts

before they are uploaded onto the network. Administration positions might also be given to CPAs, as they are independent and unbiased on the network (Deloitte, 2016). As administrators they would be tasked with vetting and checking who is allowed onto a permissioned blockchain.

Although there is much discussion on how the implementation of blockchain would change the work of the auditor and how it could make the job easier, most viewers agree that the auditor will be as relevant as it is now. Auditors will still have to apply their professional judgement to these cases and analyze how management has prepared their financial statements (Deloitte, 2016). However, Deloitte also believes that the changes are not imminent, and it will take time for them to come into effect.

As mentioned earlier, one of the most discussed features enabled by blockchains would be the possibility of real time accounting and auditing by smart contracts, and how that might change the current accounting paradigm. How these smart contracts would fit into accounting and auditing will be explained in the next chapter.

3.3. Smart Contracts

Smart contracts features have already been implemented into some blockchains, the most notable example being Ethereum, which allows users to create their own smart contracts and deploy them onto the network (Buterin, 2013). These smart contracts are powered by the Ethereum currency, but can also remit their own tokens for various purposes (fuel for the network, tokenization of assets and more) (Buterin, 2013). One example is the earlier mentioned Request Network, which has created a smart contract on the Ethereum network that has the purpose of serving as a base for decentralized applications (DApps), such as their own in-the-works triple entry accounting application (Request Network, 2018).

Although the name “smart contract” would imply that it is a form of contract is capable of being smart, it is not. A smart contract is a computer program that can autonomously approve or perform actions, provided that conditions have been met (Rozario & Vasarhelyi, 2018). A good example of a smart contract in an accounting setting is that of receiving of inventory and payment of those.

The smart contract in question would include several parts, first when the purchased inventory is received, an employee verifies and scans the bill of ladle. The smart contract reads this information, and if the ordered inventory is accounted for, it will

then release the payment automatically. In the case that the received inventory does not meet the ordered inventory, it does not release the payment (Rozario & Vasarhelyi, 2018). This would relegate the accountant to a supervisor position who monitors payments authorized by the smart contract. Combine this with accounting on the blockchain, there is a clear and immutable record that can be followed from start to the end. It has also been suggested that IoT (Internet of Things) could be incorporated with smart contracts, to for example, allow the smart contract to understand how Incoterms works (Dai & Vasarhelyi, 2017).

Deloitte (2016) provides a good example of how a smart contract could help in a derivative contract in hedging the price of oil. When an agreement has been made by two parties and they have signed a contract, it is added to the blockchain. The funds are then held in an escrow on the blockchain till when the contract is terminated. When the contract is terminated, it registers the price of the oil from an oracle, a trusted source pre-defined in the contract, and pays out to the party, who has won the bid. (Deloitte, 2016)

Potential suggestions for accounting with smart contracts are observing covenant bonds, where the real time accounting is keeping track that the terms that were set are fulfilled (Kiviat, 2015).

One of the most interesting propositions when it comes to blockchain and smart contracts, is the concept of Decentralized Autonomous Organizations, known as DAOs. These are organizations entirely governed by smart contracts (Dai & Vasarhelyi, 2017). These organizations function solely on smart contracts and have minimal human interaction. When a condition is fulfilled, it moves on to the next one. The most famous example is the Ethereum DAO, which had the purpose of dispensing Ethereum to projects. Benefits of organizations like these, are said to be the complete transparency and auditable trail of actions.

3.3.1. Automatic Real Time Accounting

In theory, blockchain and smart contracts could bring us to almost full-fledged automatic and real time accounting (Dai & Vasarhelyi, 2017). By allowing smart contracts that can automate large parts of accounting, coupled together with blockchain that offers an immutable ledger with high traceability, authors have suggested that this could be the end of financial statements (Dai & Vasarhelyi,

2017). Some experts have even gone as far as suggesting, that companies could open their accounting to interested third parties, such as stakeholders and auditors, and allow them to monitor in real time what the situation is, with the assistance of smart contracts (Dai & Vasarhelyi, 2017). This, however, is seen by many as a step that will take time to happen, because companies might not be willing to disclose everything so openly (Carlin, 2018).

Auditing could also be greatly assisted by smart contracts. In the study, “Auditing with smart contracts”, Rozario and Vasarhelyi (2018) contend that smart contracts would make the work for auditors more streamlined. Instead of actively participating in analytics and internal control tests, they could instead have smart contracts that independently and autonomously execute these actions on behalf of the auditor (Rozario & Vasarhelyi, 2018). This would give time and opportunity for the auditor to engage in other value building actions. By allowing a smart contract to take care of the audit, that independently and autonomously analyzes accounting records and other relevant information, it is believed it would be superior to the traditional audit procedure where the auditor manually selects a sample of sales contracts and likes and then by hand examines them. The same is true for smart internal control tests (Rozario & Vasarhelyi, 2018).

Kokina et al. (2017) suggests in their article that smart contracts might ease the workload of auditors significantly, by allowing automated audits processes and make it easier to track ownerships of assets by tailoring contracts. This is what could be one of the driving forces for both the accounting and auditing profession, “embedding smart contracts and machine learning capabilities into blockchain-based record-keeping systems.”, which will take care of manual and repetitive tasks (Carlin, 2018). These technological advances could greatly help push down costs for maintenance of financial records, as well as increase reliability.

3.4. Limitations and Drawbacks

However, not all agree that blockchain is suitable for the accounting environment. These exploratory studies try to show why blockchain is inherently incompatible with accounting. One of these studies is made by Coyne & McMickle (2017) who argue

that blockchain could weaken the security instead of strengthening it. One of these would be confidentiality.

In their study Coyne & McMickle (2017) are concerned that the confidentiality of blockchains are compromised when applied to accounting. On a public blockchain, all accounting information would be publicly available for everyone to see, download and edit (Coyne & McMickle, 2017). Trade secrets and other sensitive information could be leaked, creating a vulnerable environment. The authors posit that companies most likely would not be interested in having or participating in public blockchains, since they already do not want to disclose information without the explicit need for it. This raises the question whether private blockchains could be used for accounting information, since companies are privy to sharing it. This would however create problems, as the participants on the network would be very few, the auditor and company itself, which in turn leads to issues in the security of information. But in the end, the authors are not quite particularly worried about confidentiality or privacy, as the technology is constantly developing and there are already some proofs of concept on privacy and masking transactions on public blockchains.

A more pressing concern is the possibility of a 51 percent attack (Coyne & McMickle, 2017). As mentioned before in chapter 2.3.1, a 51 percent attack is when a party controls over 51 percent of the hash rate of the entire network. By controlling 51 percent, it is possible to start changing what was supposed to be immutable. For accounting to work on the blockchain, a company needs to be able to make sure that no-one can control over 51 percent of the network in order to manipulate the information on the blockchain (Coyne & McMickle, 2017). This is true for both private and public blockchains, with the public blockchain allowing anyone outside the company to potentially gaining control and the private blockchain allowing anyone inside the company to gain control. Even in a private configuration, where there is an auditor and company, the auditor might have 50 percent control over the network.

The final weakness that Coyne & McMickle (2017) mention in their paper is the incomplete transaction verification. This means that companies running these blockchains cannot verify that the transactions on the network are valid. In other words, the blockchain cannot give absolute certainty to whether something

happened in the real life, and therefore there needs to be more evidence that a transaction indeed has happened. If this is not solved, it means that fake invoices and transactions can be input into the system to inflate numbers and mislead investors and employees. Deloitte (2016) has also stated that auditors most likely will not be able to gain enough audit evidence from solely viewing blockchain transactions, which is something O'Leary (2017) also agrees with. Deloitte (2016) uses the purchase of a product paid for with bitcoin as an example scenario. In this scenario, the fact that a transaction happened is recorded on the blockchain, but an auditor would not be able to determine whether the product was delivered to the recipient, or whether the transaction was legitimate. Therefore, Deloitte (2016) wants to emphasize that transactions occurring on a blockchain can be:

- Unauthorized, fraudulent or illegal
- Executed between related parties
- Linked to a side agreement that is "off-chain"
- Incorrectly classified in the financial statements.

In other words, one cannot blindly trust what is on the blockchain, which goes against the moniker "trustless".

Rückeshäuser (2017) thinks that the blockchain is particularly ill-suited for preventing fraud at companies, due to the risk of 51 percent attacks. According to her, by giving malicious managers access to such a system, they could cover their tracks and manipulate the data according to their own will. Rückeshäuser (2017) says this could lead to situations where companies are subject to, but completely unaware of large fraudulent actions committed by one or several people, that is theoretically untraceable. Rückeshäuser (2017) does admit that this could be mitigated with a permissioned blockchain, but still believes that there is an inherent danger to it.

Another drawback of this technology is the cost of implementing it. As this is an entirely new and untested technology, those that want to try it might have to change the hardware and related underlying technologies several times. The investments can be huge and costly. If the blockchain were to be a PoW network, the electricity costs could outweigh the benefits of running everything on the blockchain, as it is resource intensive and power consuming (Coyne & McMickle, 2017). A system with PoS could potentially work better, as it is less resource intensive, but there are few

existing systems that are decentralized enough to avoid a potential 51 percent attack scenario.

People also believe that blockchain will solve all problems, but it in fact will not solve all issues. A blockchain will not prevent misappropriation, as it only is a tool to convey information. Correcting potential accounting mistakes might become harder to accomplish, as the information is now immutable. On the other hand, it also can lead to creating a false sense of security among people relying on the accounting information from the blockchain.

Although not a direct drawback or limitation, the interest in researching accounting functions on the blockchain has remained very lackluster, even though there have been promises that the technology will provide major improvements over the current double-entry accounting system. According to Carlin (2018) this would be the perfect time for accountants to help shape the future of their profession, be it in regulation or practical application. Furthermore, Carlin believes that triple-entry accounting on the blockchain has potential to change the industry, but the window of opportunity to influence the future is now (2018). If we do not seize the opportunity to create a standardized solution for accounting and auditing on the blockchain when the technology is still being researched and developed, it will lead to a fractured approach in the future, in addition to a lack in regulation (Carlin, 2018).

Blockchain is still an untested technology in the accounting field. As of right now, there are no studies on whether blockchain will save money or if it will be costlier to operate. These are all facts that make it hard to determine at this point if it is a good investment from an economical point of view or not.

4. Methodology

This chapter is dedicated to presenting the methodology, hypothesis and approach. In this chapter the foundation for answering the question asked by this master's thesis, "what are the Finnish auditors' receptibility to blockchain in the accounting/auditing industry", will be detailed. Since this a new field of research, there is not much quantitative data available, which in turn indicates that this thesis must be a qualitative study. No prior studies have been done in Finland, asking auditors on their thoughts on blockchain.

4.1. Qualitative

To be able to assess whether the qualitative research has a high enough quality, we need to measure the reliability and validity of the study. Reliability can be divided into two parts: external reliability and internal reliability. External reliability is a measurement on how well a study can be replicated. However, this is difficult to measure in qualitative studies, as social settings cannot be frozen and are always evolving (Bryman 2015). This is also applicable to when researching something that is currently developing or emerging. As time goes on, opinions and thoughts will develop over time, as Lampard and Pole (2015) put it; "the data yielded are a reflection of the circumstances under which the interview is conducted." We also arrive at another issue when discussing internal reliability, which requires there to be more than one observer or member in a team that agree on what they see and hear (Bryman 2015), however this is of course becomes problematic when only one person is conducting an interview. According to Bryman, this can be addressed by displaying the research process, choice of theory, field notes and so on, to allow others to reproduce the research as close as the original as possible.

Validity refers to "you are observing, identifying, or "measuring" what you are seeing". Just as with reliability, this can be divided into internal and external validity. Internal validity refers to the idea that there is a good connection between the observations of the researcher and the theoretical ideas. According to Bryman (2015), this is the "strength" of qualitative studies, since it gives a much closer understand and viewpoint of the subject that is being currently studied. External validity is, however, an issue for qualitative research, as it refers to "which degree the findings can be generalized across a social setting.". This is usually a lot harder

in qualitative studies due to the small sample sizes used in these studies, either in ethnographic or case studies.

4.2. Hypothesis

The purpose of this study is to measure the receptibility of auditors in Finland, relating to blockchain. This is one of the first if not the first ever studies in Finland that has been done to gauge the interests and receptibility of auditors, in relation to blockchain technology in the context of accounting and auditing. Therefore, this will be an exploratory study.

Based on previous studies done abroad on the perceived impact of blockchain in the accounting and auditing industry, most authors believe there will be some form of change from blockchain. There are therefore two different hypotheses' concerning the auditors receptibility of blockchain:

> H1 Auditors expect that the promise and underlying technology of blockchain and distributed ledger technology will change how accounting works.
>
> H2 Auditors expect that the promise and underlying technology of blockchain and distributed ledger technology will change how auditors will conduct their work in the future.

In other countries, auditors are already receiving training in what blockchain is and how it functions, it would not be surprising to see this phenomenon eventually in Finland as well. Therefore, auditors might already have a certain expectation on what blockchain could mean for the accounting industry and the auditors' work. It is not completely unwarranted to believe that the auditors believe there will be some form of change to the industry, based on the research that has been done by academics.

There are several forms of qualitative approaches we can take, but for this research, the best approach for a qualitative study is to conduct interviews with auditors. The idea is to use the results of the interviews, which are non-structured, to gain a better understanding of what participants know about blockchain technology and its relation to the accounting and auditing industry (Walle, 2015). The next part will explain the data and sources, as well as how the interviews will be conducted. Later, interviewing will be explained as well.

4.3. Data and Sources

In other countries, the Big 5 (KPMG, Deloitte, PwC, BDO and EY) are researching future applications of both accounting and auditing on the blockchain, which is one of the reasons why the Big 5 also would be the main group of interest in this research. The best approach to get reliable data is to use a homogenous population (Walle, 2015).

One of the issues, when researching new phenomenon's or technologies, is the lack of awareness. People are most likely very aware of Bitcoin, but are they aware of the underlying technology? Do they understand it? Therefore, it might be a good idea to include an explanation on what blockchain is, if a person has answered that they are not aware of what it entails. This, however, does bring up the potential danger of contaminating the people participating in the survey (Walle, 2015).

The alternative is to provide examples of different scenarios and explanations on what is being asked, however the issue here is that the questions might be incur a bias in the respondents (Walle, 2015)

Another question is whether the questions should be limited to simple scales from one to five, or if we want respondents to respond to the question with their own answers. The benefit of having a simple scale is that the information is much easier to quantify, as there are preselected categories (Walle, 2015). However, if we let the respondents respond with their own answers, there is a potential of receiving more in-depth answers to the questions that are being asked (Walle, 2015). This does lead to a potential issue where it might be harder to quantify the data, but the method suits much better to what this study is trying to accomplish.

To acquire the best information possible, both current and former auditors will be asked to participate. Only auditors with two or more years of experience will be considered for interviews. We want the auditors interviewed to have some form of working experience of the industry. As for former auditors, we want them to have been out of the job for less than five years. By having older and more experienced auditors in our data samples, even those who have quit the job or that are retired, we will gain insights from those where the industry has been heading and who have a more intricate understanding of how the auditing and accounting industry works.

Through a combination of auditors with different amounts of work experience we have a better understanding of what auditors think of blockchain in an accounting and auditing environment. The young auditors might be more open to new technologies, whilst auditors in the middle of their career understand what the current trend is. The former auditors, especially recently retired, have a deep knowledge and understanding of the auditing industry are likely able to see whether the industry would want to use a technology like blockchain.

4.4. Interviews

Interviews always consist of two parties: The informant and the investigator (Walle, 2015). The informer is the one providing answers to the investigators questions and depending on what kind of an interview it is, will respond to the questions in a predetermined way (Walle, 2015).

For the interviews to be effective, the informant needs to be somewhat familiar with the interview area (Walle, 2015). In this case the area would revolve around blockchain, accounting and auditing. As a graduate in accounting the interviewer has experience in the area that will be interviewed in, but there are no guarantees that the persons selected will have any experience in the blockchain area I want to interview them about. Therefore, information needs to be supplied to the interview candidates either before or at the start of the interview, or I must forego all auditors, who have no experience of blockchain technology, and try to find only those who have some experience.

Deciding to exclude or include those who have no experience comes with certain challenges, benefits, and drawbacks. The first major challenge would be finding enough people who have experience or a good understanding of what blockchain is, and how it could be used in an accounting and auditing setting. Finland is a small country, but we have highly educated auditors. However, since blockchain is a new technology, the number of people familiar with the technology might be rather low. This is the reason that auditors who have no have little to no experience about blockchain have been included, there might simply not be enough auditors who are knowledgeable in this area, and as this is a study to measure receptibility and thoughts on this subject, even those who are not experts should be considered.

One of the benefits of including people with little to no experience is also receiving ideas and viewpoints from people who are not as well versed in the subject. It is a double-edged sword, as they might provide insight that is very pertinent to the thesis, but on the other hand they might not be able to give any data that can be used for this research.

In this case, participants both without and with forehand knowledge of blockchain could participate. This answers one of the research questions, whether auditors know about blockchain technology. The answer to this was collected when asking the auditors whether they wanted to participate in an interview about on accounting and auditing with blockchain. They were also asked if they are aware of what it is.

Those that wanted to participate were sent a short primer on what blockchain technology is. This guide was sent to all participants, no matter if they had answered

if they knew what blockchain is or not. The guide has been provided as an appendix (appendix B). Walle (2015) provides in his book a good guide on how to structure an interview to have it be efficient. The first step is to establish goals of research, which we already have. We want to know what auditors know about blockchain and if they believe accounting will benefit from it.

ISSUE	**ANALYSIS**
Establish goals	What is the purpose of the research? What kind of information is needed and why?
Research/background	Conduct secondary research to insure that the interviewers have the knowledge to ask the right questions and spontaneously follow-up.
Prepare questions	Focus upon both the substantive information sought and the format to be used (such as structured or open-ended questions).
Strategic order	Ask the most important questions as early as possible. Create a flow so questions build upon each other in synergistic ways. Keep sensitive questions last.
DISCUSSION Preparation can be complicated. It begins with an understanding of what information is needed. This is followed by developing questions and ordering them in a strategic manner. At that point the research can begin.	

Figure 5 Walle

The second step is to make sure that the material understood well enough by the person conducting the interview, so that they can ask questions that relate to the area they want to research.

The third step is preparing the questions once the purpose of the interview is understood. Depending on the structure of the interview, the questions change.

The fourth step is related to organizing how the questions are asked. The most important questions should be asked first, and questions that are not as relevant as last

At this point, it should be clear whether it will be an unstructured or a structured interview. This thesis will rely on a semi-structured interview with pre-established questions, that are open-ended, allowing for the informants to speak their mind and give their honest opinion on the topic at hand (Walle, 2015). In this case a semi-structured interview is better, since it gives the interview a structure to follow for both the investigator and informant. But the semi-structured interview also allows the investigator to ask questions outside of the interview guide, which gives more flexibility and can lead to interesting discoveries, even though one is still following the same general thread as the other interviews (Bryman & Bell, 2015). If possible, these interviews would be face-to-face, but phone calls and skype are also alternatives as it depends on what the informant can do.

For this interview, people with and without working experience of blockchain have been interviewed. This is a new field and there have been very few projects developed in blockchain at Big 5 companies. Therefore, participants without experience are a valuable resource to understand the implications of blockchain.

4.4.2. Interview Guide

Before conducting interviews, an interview guide needs to be developed. The interview guide gives direction to the interview and allows the interviewer to focus on asking the correct questions from the subject. To develop the questions that were to be asked of the subjects, previous studies needed to be analysed and let them influence the most important questions related to the main purpose of the thesis (Walle, 2015).

In the case of this thesis, there are not many articles written on the auditors' perceptions on blockchain in an accounting and auditing environment, and there is none in Finland so far. This is not a bad case, as this allows us to perform research about something almost completely new, and from a Finnish perspective. This in its turn means we must develop the questions from a blank slate and extract the most important parts about blockchain and those that might interest auditors.

To make sure the interviews are as fluent as possible, we want to group these interviews into different categories. This should allow the conversation to flow unimpededly, combined with the interview being designed to be a semi-structured interview. Although the interview guide should, indeed, be a guide for the interview, the open nature of a semi-structured interview allows the interview to explore areas that would not be discussed when only utilizing structured interview and this might lead to new areas that should be studied further (Walle, 2015). However, this can cause issues if the interview does not control the discussion, as it might generate information that is unnecessary and causes extra work when coding and analysing the information.

After the interview guide is developed, it is important to test it and further refine it, and hence a pre-check was conducted. This pre-check interview was used to change and adjust some questions, as well as improve the quality of the questions. The pre-check interview was not included as an interview, as the interview questions were changed enough for the answers to no longer be relevant for this thesis.

4.5. Conducting Interviews

For this interview, nine people with different levels of experience from financial auditing were interviewed. These auditors were contacted through several means, some were personal connections, others were reached through the help of other participants and some were contacted on social media and asked if they wanted to participate.

In this case, since we wanted to see the receptibility of auditors on blockchain in Finland, and their knowledge, searching information from both those who have heard about it and not heard about it, there was not a strict criterion on prior knowledge. An introductory letter was sent to all participants detailing the purpose of the interviews

and giving a short explanation on what blockchain is. As mentioned earlier, this letter is appendix B in this thesis.

4.6. Data Saturation and Analysis

When it comes to qualitative studies, especially interviews, it is usually not as straightforward to find the number of people that should be interviewed. The most common and simple method of finding the right number of participants is to first agree on a number that one thinks would be enough for the interviews, the sample size. Then one needs to look out for “saturation point” (Saunders et al., 2018). This is a crucial point, as this is the point that determines when enough interviews have been carried out. The saturation point, in its simplicity, means that a suitable amount of people has been interviewed so that conclusions can be drawn from the data available and that no new information can be expected from consequent interviews (Saunders et al., 2018). It is not recommended to interview one or two people and say that the saturation point has been reached, as that does risk the pool being too small, and will skew the results massively.

The point of interviewing people up to the saturation point and not beyond, is that no new additional information will be supplied to the research, and the more interviews will only be additional work, for no real pay-off, Fusch (2015) calls this “depth in data”. Data collection for qualitative studies is not about the numbers of participants, but about the amount of information collected from the participants. One should aim for a combination of so called “thick” and “rich data” (Fusch, 2015). This means that you preferably want “thick, as in “a lot of data” and “rich data” which is nuanced, intricate and more. This allows for a better and easier analysis of the material. In the case of this thesis, a lower number of interviewees was also wanted, as the questions were open ended and meant to spark a conversation. The saturation point was reached quickly, as the knowledge of this area is still quite limited in Finland.

Saturation point analysis with a small sample size is not as statistically rigid as ANOVA, nor does it allow us to draw any definitive conclusions on what has been uncovered. This is a compromise that must be considered when conducting an exploratory study on a new topic, as the sample sizes can be expected to be small due to the lack of available expertise or material in Finland.

The interviews will be transcribed making the answers provided by the auditors accessible for easier analysis and readability when analyzing the data. Once the interviews have been transcribed, a simple matrix of ‘yes’ and ‘no’ responses can be created, which allows for a quick analysis of what auditors think of each question.

5. Discussion on Findings

In total nine auditors were willing to participate in the interviews revolving around blockchain, accounting and auditing. Although the sample size is small, it does allow us to draw conclusions on what is the purpose of this thesis: what is the receptibility of auditors in Finland related to blockchain, and what they think of the technology. As stated in the methodology chapter 4: when conducting research where interviews are the main method of discovery, the number of interviewees is not set in stone, and instead focus should be on finding a pattern from the responses (Saunders et al., 2018). In this case, interviewing the nine people that were willing to participate has resulted in enough material to identify trends and visions of what auditors think of blockchain, and how they see it impacting the accounting and auditing industry in the future.

All the interviewed were from the Big 5 accounting companies, some were recently retired, but most of them were still in the workforce. A breakdown is provided below. The auditors taking part in the interviews have been given pseudonyms for anonymity, and gender has also been swapped on some of the participants.

Name of participant	Years of experience
Martin	2-10
Johanna	21-30
Peter	21-30
Thor	2-10
Johan	2-10
Per	21-30
Stefan	31-40
Stella	2-10
Carl	11-20

The participants who agreed to be interviewed varied greatly in years working with auditing. The subjects were chosen through purposive sampling. The goal of purposive sampling is to find subjects with rich stories that are required for the study.

Some of the auditors had also pivoted towards IT-auditing after working with financial auditing for a while. One auditor had not worked directly as a financial auditor but supported them and had worked his entire career as an IT-auditor. The reason for the inclusion of this auditor, was simply because blockchain is at this point mostly a technical solution. Therefore, it was important to hear the thoughts of an IT-auditor, on this technology and how it could function in an audit environment.

The interviews were conducted in several different ways. Five were interviewed at their offices, three were interviewed over phone or skype and the last one was interviewed at a coffeeshop.

5.1. Interview Questions and Answers

As mentioned in the methodology chapter, the respondents were selected based on different categories of years of work experience. The purpose of this was to find participants who can provide different opinions, influenced by their years working, but still working in the same industry. People who have been working for longer periods as auditors have seen more changes come and go to their work and are important in analyzing whether blockchain has the potential to introduce something new and useful for both accounting and auditing. However, interviewing auditors who have been working from two years up to ten, is also an important demographic element in the study. These auditors are the future of the field and are the ones who might be working with this kind of technology. Therefore, it is of paramount importance why they needed to be interviewed. Same goes for the participants with over ten to twenty years of experience, these are the future managers (if not already managers) and some of them will be participating in and driving changes at the Big 5 accounting companies.

Below is an analysis of each of the question directed to the auditors with some of the comments they added after they were probed.

5.2. Analysis of Questions

The questions presented here were created with the expressed purpose of measuring the auditors receptibility on blockchain, and other thoughts. These questions vary from the very basic fundamentals offered by blockchains, on whether the immutability of blockchains can increase trust or reliability of accounting records. Some of the questions try to measure whether smart contracts are something auditors believe they would have use of, and another asks whether auditors expect that their jobs would change if blockchain technology would be implemented by their customers and into their own jobs were also asked. Each question below has an explanation as to why they were asked. An appendix (A) with the questions has been attached.

Question 1. Have you heard about blockchain before this interview?

This question was devised to measure whether Finnish auditors had heard about blockchain before this interview. If they had heard, they were further probed on, in what context they had heard of it.

Out of all the participants in this interview, six out of nine auditors had heard about blockchain in one form or another. Johanna, Thor, Johan, Per, Stefan and Carl were the ones that had knowledge before they were sent the explanatory letter introducing this interview and what blockchain is.

With further probing, it was discovered that Thor, Johan, Per, Stefan and Carl had all gained knowledge about blockchain technology through discussions with colleagues on virtual currencies, meanwhile Johanna had heard about it being discussed at client companies. Both Johan and Per had further read about the subject; Johan attended lectures on the subject, whilst Per read studies done by the company that he works at.

Question 2. Has your company or colleagues expressed interest in blockchain?

This question was asked to measure the general knowledge among coworkers and at the workplace on blockchain technology. By analyzing this question, it is easier to understand what kind of an interest there is among the accounting companies, and if they think that the technology could be beneficial for them or their clients. The weakness in this question, is that it does not measure actual development, and it also does not consider what the IT department might be working on without the auditors' knowledge, that might be related to accounting and auditing on the blockchain. Another issue is that auditors do not necessarily talk about technical solutions to auditing, and instead discuss more general work-related matters.

Nonetheless, discussions with colleagues can grant us a good understanding on what the current sentiment at the company is and they give us the chance to further extrapolate on what the current thoughts are in the industry.

Only three out of the nine interviewed said that they had heard their colleagues talking about the technology. Johanna mentioned that in her case, it had been the consultants who had expressed interest in the technology. Johan, on the other hand, who has closer contacts with the IT department, mentioned that they had discussed with colleagues what kind of an impact blockchain could potentially have on both accounting and auditing. They also mentioned that most likely every single Big 5 is taking notice of blockchain and trying to evaluate what the impacts of this might be for the future of auditing and accounting.

Carl, who works as an IT auditor, and has been working closely with auditors through his entire career, mentioned that in their team they have been discussing blockchain on a technical level and potential future use-cases for the technology. Johan mentioned that in their case, they had been discussing the valuation of cryptocurrencies, not the application cases of the blockchain technology.

The responses to this question are unsurprising since the technology is still very nascent, but there has still been discussion about blockchain technology. The most important takeaway and conclusion from the responses, is that from those working with auditing related matters, have not seen an interest from their workplaces of implementing it to accounting or auditing.

Question 3. Will immutability increase reliability of accounting information?

The immutability provided by blockchain is one of the most important aspects of the technology. By asking auditors their opinions on whether the accounting entries would be more reliable and accurate in practical life, we should be able to gauge how important they believe this feature is and whether it is something that they would value having in their line of work.

When asked about immutability provided by blockchain, there was a split on whether it would in fact improve reliability of information. Johanna, Stefan, Stella and Carl thought reliability would benefit from immutability provided by the blockchain, by for example, having machines automatically enter information could potentially be more reliable than having a human enter the information. They did however admit that a human would be needed to supervise it in some way to prevent egregious mistakes from happening. Stella mentioned that “one of the purposes of auditors is to verify the reliability of data, and make sure it hasn’t been tampered with.” She then mentioned that being able to have the power to make sure information is reliable without having to separately vet it, would decrease the auditors’ workload. Johanna mentioned that immutability would, in her opinion, increase the reliability and would require less manual checking.

Martin, Peter, Thor, Johan and Per expressed another opinion. Although they saw benefits of having information digitized, easily accessible and immutable, it would not make information inherently more reliable. There could still be issues when entering the information, i.e. entering wrong information, entering fraudulent information or not entering certain information. The reliability of information is based on the data that is entered, and the people entering it. Therefore, it would not be inherently more reliable. With the information being immutable, it would be much harder to change the information afterwards in case it was wrong. Having information on the blockchain does not mean that the information is more reliable, some of the respondents had added.

The ones for and the ones against both raise important points, and the participants arguing against it increasing reliability, are correct in their viewpoint that the weak point of course is the stage where information is entered. Peter put it quite succinctly, “nothing is bulletproof and completely secure.”

Question 4. Will immutability increase trust of accounting information?

This question was asked because one of the aspects of blockchain is its "trustlessness" which should increase the trustworthiness of the information that exists on the blockchain, by not requiring any central authority to preside over the data. In the context of accounting and auditing, the immutability of information existing on a blockchain could technically increase the trustworthiness of the accounting process.

Most of the interviewees did believe that the immutability could increase the trust of accounting information. In their answers to this question, everyone except Martin and Per agreed that trust could increase due to the immutable aspect. When probing the auditors that thought that immutability would increase trust, they said that having the information locked down and immutable after being entered, would help them know that the information cannot have been tampered with after the fact. This does not of course exclude fraud, as some of the interviewees said, since the bookings still need to be verified to have been done correctly.

Carl, Johan and Per, who had read about blockchain more extensively, mentioned that since information could be changed later by adding or subtracting wanted sums, it would still be quite safe from manipulation and trust of the information would be high. They based their view on the fact that there would always be an untamperable chain of events. The issue of entering false information persists, they said, but the fact that the entire system is based on being "trustless" would hopefully mitigate this issue.

Question 5. Would corporations prefer private or public blockchains?

The purpose of this question is to understand whether corporations would prefer a private or public blockchain from the perspective of an auditor. Auditors are in the position to give their opinion on whether their clients would prefer to use a private or public blockchain if they were to use blockchain for their accounting. This is a question that goes into the heart of what a blockchain is, should it be a private or a public blockchain, since it dictates how safe it is and who has access to it.

As can be seen in the results, every single auditor said that private blockchains would be the most preferable alternative. When probed about this, the answers they gave were straightforward. There is a lot of sensitive financial information being passed around, and if a blockchain would be public, this information would be open for everyone to see. Although this information is obfuscated with random hashes, the accounts that money would go into would still be open for everyone to see. Peter, Carl and Johan mentioned that some of the accounting information could be put on a public blockchain for investors to access and use when evaluating companies. Peter also added that this could also be compromise for when authorities need to look for information, as they would just need to look for the information they need and when they need, instead of having the accounting department conjure up the information for a specific request.

Johan mentioned that consortium blockchains would most likely be the perfect middle-path for companies, as they would be on large network which would mean less chance of tampering and there would be less maintenance costs due to, hopefully, a third-party taking care of the network. However, companies might still be worried that the sensitive information could be seen by competitors and they would not be in control of everything. Hence, Johan also suggested that companies most likely would start off with private blockchains and could potentially move to something akin to a consortium blockchain in the future.

Expectedly, private blockchains are what all respondents suggested that companies will be using. This makes sense, since private blockchains are as their name suggests, private. However, the usage of private blockchains can defeat the purpose of blockchains, as they are usually owned by one party. Encryption could be a future solution for keeping information safe on public blockchains, and there are some in the works for the Ethereum blockchain.

Question 6. Would information in real-time would be useful for auditors?

This question has the purpose of establishing whether the real-time nature of blockchains would be of any use for auditors. This is one of the fundamental benefits of blockchain since information can be appended to a blockchain instantaneously. This in turn can create a real-time stream of accounting information. Considering

this, auditors might be able to follow up accounting information in real time and take snapshots of the current situation of a client.

Most of the auditors thought that this information processing would bring some form of benefit to both reporting from companies and it would also help when auditing. When probing further into why they thought this solution would help with auditing and reporting, Johanna, Johan, Stella and Carl said that it would change the way we need to think of auditing. Not having to wait for information to be updated and bookings to be made, would make information be available instantly. This would slightly change the role of the auditor from looking into the past and looking at the present instead. However, the auditors who reflected this opinion still said that auditing will remain mostly focused on looking at the past, since it gives a more complete picture. Realtime auditing might speed up the process of consolidating information, which in turn would speed up auditing.

Martin and Peter, who did not think real-time information would help, simply said that auditing looks at the past and will remain like that. They did not see any additional benefits from having access to real-time information. If someone were to try and utilize it for auditing purposes, as in real-time auditing, there would be too much information to filter and process to be useful.

Question 7. Can digitized/distributed information from the blockchain ease auditing work?

Information on the blockchain is always digitized and available in a distributed manner. In the case of a blockchain, in case one source fails, the same exact information is available from other nodes on the blockchain. As mentioned earlier this feature is what sets blockchain apart from other forms of digital storage that function with one centralized operator.

When asking the auditors on whether they believe that digitized information on the blockchain would be to any benefit in auditing, every single person said yes, that it would.

When probing them on why they thought that auditing could benefit from this, Martin, Johanna, Thor Stefan, Stella and Carl stated that digital and digitized information is

already part of their job and they extensively use it when the time comes to conduct auditing. For example, receipts and other documents that are used in auditing come both in digital and physical form. The digital format was preferred by the auditors as it made their job faster and easier, without having any need to have someone from the client fetch the material from storage, when conducting audit work. With their understanding of blockchain, they liked the idea of having all the information on the chain, always accessible. Johanna and Johan mentioned that it would be convenient to have the information available at their workplace through some form of connection to the clients blockchain. A lot of the auditing work could be conducted at the office instead of travelling to the clients. Johanna also mentioned that this would also decrease the preparatory work done before the audit, as auditors could check transactions and receipts and records with the corresponding hashes, and this coincides with what some of the previous studies state. Johanna and Johan said that with some clients, they already have access to digital records straight from their workplace, but they are still quite rare.

Question 8. Are accounting smart contracts a good idea?

With smart contracts being an increasingly important part of blockchains, the auditor's opinions on these are important to measure, as they are the part of the blockchain that can help auditors to complete audits both faster and more efficiently. This is also true for accounting departments that could see a potential boon from an automated system akin to smart contracts.

When asked about smart contracts in the case of accounting and if they would assist their clients with accounting, most auditors were in favor it. In general, automation is something that the clients are already striving to use, but it is still some ways off. Some of their clients use very rudimentary automated systems, for example booking products coming into warehouses and adding these to the balance sheet. However, the payments still need to be done by a human. Automating accounting with simple smart contracts could potentially allow for faster accounting at finance departments. Peter stated that simple transactions could easily be handled by smart contracts, and possibly even be of assistance in complex transactions. Martin mentioned that

allowing accounting smart contracts could assist in reducing cost and overhead in the accounting departments.

The danger is to rely too much on automation, according to a couple of auditors. Automation is a nice “cushion”, as Peter stated, that allows people to focus on more complex bookings, however, it can also mean that people no longer critically think of simple transactions and let them run their own course. This has the potential for abuse, and a safeguard should be to always require someone at least to monitor the transactions in case there is something that raises suspicions. Another risk, asked as a question by Martin, is what happens if an invoice is wrong and paid? Since it is on the blockchain, it cannot be rolled back, it is a permanent addition to the network. Stella wanted to emphasize that this new system would put a lot more responsibility on accountants to check whether the information is correct and be constantly vigilant, however the amount of human-made errors would decrease, if not almost completely disappear.

Question 9. Are auditing smart contracts a good idea?

For auditors, auditing smart contracts on the blockchain have the potential to help auditors to analyze the simplest transactions automatically, but more complex transactions would still require auditors to either analyze them together with the smart contracts, or to do it manually. These smart contracts, however, can be tailored to suit their current client.

The auditors agreed that smart contracts would make life at least a bit easier. Having small software programs that perform basic auditing when auditors are analyzing the more complex transactions would decrease the workload. This would also potentially be a cost savings move as well, since demanding fewer people to analyze transactions, less people would be needed in general.

Stella and Martin mentioned that they did like the thought of being able to adapt a smart contract depending on the job. Thor stated that time could be spent on value building, customer relations and testing internal systems more efficiently and more robustly, with smart contracts taking care of the simple transactions. Johanna suggested using smart to solely focus on more complex transactions and Carl

suggested that smart contracts could be used to verify receipts and other documents.

Although there is already some form of automation employed in some audit tasks, smart contracts would take it a step further, streamlining basic processes. However, this would not make auditors obsolete, as they are still needed for evaluating the more intricate and complex transactions that a computer system would not be able analyze. These would be for example, anything with any component of valuation. Not all tasks can be automated as said by Stefan.

Question 10. If blockchain were to be implemented, will it change the auditing job?

Considering that blockchain is being touted as a revolutionary technology that will change many industries, it is of interest to understand whether the auditors themselves believe that the technology will change how they work. The interviewed auditors have had some time to understand what blockchain is, in form of the introductory letter.

Most of the auditors believe that auditing would change if blockchain were to become a standard used at companies. When asked why they thought so, Johanna, for example, mentioned that auditing would become much more technical in nature. Carl and Johan who currently work as IT-auditors stated that there are a couple of possible outcomes. One is that financial auditors might have to learn programming languages to be able to interact with blockchains, in addition to being technically literate in general. The main reason for learning programming languages would so that one could interact with smart contracts on the blockchain. This knowledge would allow auditors to tailor-make contracts to extract information from the blockchain to use in auditing. Johanna mentioned that if the blockchain would live up to its promise, more time could be spent on analyzing complex transactions, and let smart contracts take care of the easier one.

Johanna mentioned that this procedure could also give the birth to several other new forms of auditors, one being smart-contract auditors. These would be auditors who have been training with and have experience in checking the status of smart

contracts. Their purpose is to assure that smart contracts going live will not have any vulnerabilities or serious faults. In general, the entire industry is moving more towards data-analysis and IT related functions, meaning that the impact of blockchain would have to be separately observed.

Martin, Peter, Thor and Per agreed that blockchain would change their jobs, but, were not able to specify how. They all stated it is too early to say how it will cause changes, but when implemented it would change their job description.

Of those participants, who disagreed, Stefan and Stella, stated that the auditor role will not change, and it will remain the same. The role of the auditor will always be to look back at past events and making sure that they have been executed correctly and that everything is fulfilled according to the legislation. The auditor is too important as they are now for the role to change.

Question 11. Do you perceive some fundamental weaknesses in blockchain?

The purpose of this open-ended question is to understand what kind of worries the auditors have with this technology.

Most auditors believed there are some forms of weaknesses in blockchain. Most of these were related to how one would make sure that information entered is to be completely trusted. Martin, Johanna, Peter, Thor and Per did admit that the information entered now suffers from the same issue. But since blockchain is supposed to be trustless, it really would require new thinking and complete trust in the technology. Per said that he does not believe the blockchain will ever be completely independent, and it will only truly work if it is being supervised. Johan mentioned that to completely work as intended, all control would have to be transferred to the blockchain, and this is something he did not think would happen.

Stella mentioned that it will be interesting to see what an effect the EU General Data Protection Regulation (also known as GDPR) will have on how blockchains work in the European Union. One of the requirements of GDPR is that all information that companies or service providers have of customers, can be requested to be deleted by the customer. This goes completely against the philosophy of the blockchain, where everything is permanent and immutable. However, it is worth noting that the

European Union has founded the “EU Blockchain observatory and forum”, which serves the purpose of helping and accelerating blockchain adoption in the EU. Therefore, the EU will most likely be looking at solutions for problems like Stella mentioned.

Question 12. Do you have any other comments?

The last question was important, because it allowed the participants of the interviews to convey feelings, thoughts and opinions that the interview questions might not have captured.

Johanna, Johan, Per, Stella and Carl stated that this is an interesting development, and they wonder how this technology will change their jobs and if it will change during their lifetime and career. Johanna, Per and Stella stated that this issue is a bit too technical for them, but they said that the field is changing constantly. Johan mentioned that the auditing field in general is moving towards a more data driven audit future. This means that by using multiple sources of data and combining them when conducting audits, it would help reduce the workload as well as streamline the tasks they already are doing.

Johan who has transitioned into IT auditing mentioned that in the future, financial auditors will need to be more well versed in blockchain and understand how it works. Johan also mentions that there might come a point where financial auditors will not be able to work with auditing, without the knowledge of how blockchains work, and the programming languages they utilize. This would put a large emphasis on future education for future auditors. However, this does not mean that current auditors would be left without a job, as the transition period might be long to get all customers onboarded to such a system.

Stella mentioned that it is a fascinating technology, and that the single aspect that interests them most, is the transparency that blockchain could provide to both accounting and auditing.

Another opinion was presented by Johanna who thinks the technology will be adopted eventually, but that the change will be positive. She didn’t have any idea of how long it would take for blockchain to proliferate in different industries, but she

mentioned that it would take longer for conservative industries and companies to accept a potential change in the status quo.

6. Conclusions

With reference to the interviews conducted, and results shown in the previous chapter, the conclusions of this study can be presented in this chapter. By analyzing the answers from the interviews, we can see that Finnish auditors working at the Big 5 auditing companies have expectations that there will be substantial changes if blockchain technology were to be implemented into accounting and auditing.

Considering that blockchain is still a very new technology, the expectations that auditors would be familiar with the technology were not particularly high. However, most of the participants in this study did in fact have knowledge about blockchain prior to this interview. Perhaps not unexpectedly they had heard about it in the context of cryptocurrencies, mostly bitcoin, related to how these should be presented in financial statements. Even those participants who had been asked if they were interested in participating in interviews, but declined, mentioned that they had heard about blockchain, but they did not feel comfortable participating as they did not think their knowledge would suffice in giving good enough answers.

One of the more notable aspects was how the auditors taking part in the interviews quickly understood the basic concepts of blockchain technology and were able to give good insights into how auditors in the field would embrace this technology, as well as considering if companies would be ready for a shift in accounting.

The introductory letter sent to participants when they agreed to take part in the interview only served as a basic primer for the interviews. It did not contain any of the more complicated and nuanced viewpoints that some of the auditors expressed. Many of the expressed opinions fell in line with what the academic papers have suggested would happen. As an example, one suggestion was that auditors would want to use smart contracts in assisting with checking simple transactions, and they themselves focus on complicated transactions as well as value building activities.

In addition to smart contracts playing a larger role, added security of blockchain to accounting records was considered important. There was a split in views regarding whether the respondents expected that immutability would in fact help to add reliability of information. Trustworthiness on the other hand was universally agreed on, would increase with blockchain. This is quite in line with the academic studies,

where it has been expected that accounting and auditing will strongly benefit from the technical solutions that blockchain can offer.

In general, it seems like auditors are expecting changes to both accounting and auditing if blockchain technology becomes the future standard. This would also change how both accountants and auditors work. It is too early to say how it will alter their jobs, but they see some changes coming, varying from total disruption on how the career works, to changes only in the technology they use to conduct their current jobs. However, it was also interesting to see that some auditors believed that the role of the auditor would not change, as they are there to give assurances to stakeholders and they will retain a role that looks at the past and not the present.

It is important to acknowledge that since blockchain is such a new technology it could not be expected from the participants that they would understand how the technology works from the information provided in short introductory letter. Like of the participants said, “auditors are not well versed in understanding how the technology they use works”, which could also be true for if auditors would be working with blockchain technology. However, it is also possible that this would not be the case, as the structure and functions of the blockchain is interwoven with how accounting and auditing would work on the platform, compared to how it works today without blockchain.

For blockchain to become an accepted technology that can be used in both accounting and auditing, a lot of work needs to be put into understanding the usage in those contexts. IT auditors will learn how blockchain works on a technical level and then co-operate with financial auditors on how it could be utilized for accounting and auditing. This should be combined with teaching financial auditors how blockchain functions, to help them to better participate in building a framework for how blockchains should be utilized. The Big 5 could also offer more general education in this area, if the major companies believe it would be something that the auditors will need to learn. There are already Big 5 branches abroad that offer education regarding blockchain, but we are yet to see that in Finland.

Blockchain is a nascent technology and it is unknown if it will truly be as revolutionary as some are expecting it to be. Of the interviewed auditors, most seemed to think that the technology has a potential, but all these views are based on

theoretical discussions and not data-based examples. None of the auditors had worked with blockchain ‘hands-on’, but some of them had researched it before they were asked to participate in the interview. One of the auditors stated that the largest issue with getting blockchain implemented, is that there is a lot of talk, but few are doing the actual construction work. A major reason for this might be, that blockchain has only existed since 2008. Another issue is of course the cost of investing in a completely new technology, which is almost always more expensive than preserving the incumbent technology. However, Finland could potentially be a good market to test this technology, since the country is a small market with high IT-prevalence.

A view pointed out by another interviewee, was that it will be hard to get more conservative industries to move to a new form of accounting. This conclusion in its turn raises another question: Would there be a world where both double and triple entry accounting exists? There are plenty of organizations that do not need triple entry accounting and they could survive using double entry accounting, but could it be possible that triple entry accounting would become mandatory for all organizations?

With blockchain development currently still at an early stage, it is up to the accounting companies to try and learn and to see what benefits they can get out of it. Independent actors are important contributors to the future of blockchain and should not be understated. Accounting companies can have a large impact on how this technology will be utilized in accounting and auditing and help develop the field at this early stage, and will potentially be very important in helping to realize how legislation will affect accounting and auditing on the blockchain, but the time to act is now if the companies want to shape what accounting and auditing on the blockchain will look like.

6.1. Limitations

Although this study managed to answer the questions that were posed at the start of this thesis, there are shortcomings. One of these is the number of participants for this study.

This study had nine participants, and one test candidate to improve the answers. Although a saturation point was reached, it would be optimal if a future study had more participants to receive more answers. The limitation in this case was that

people do not seem to be comfortable to talk about blockchain, since they are not completely knowledgeable on the subject. This is very understandable, and fortunately people, who did not apparently understand or know of blockchain were willing to participate. With this limitation in mind, it also means we can not draw any definitive conclusions.

6.2. Future Studies

Based on the results of this study, there is a couple of recommendations for future studies. One of these is to elaborate a questionnaire to get a larger sample of the auditors. There are a few ways to do this. One suggestion would be to wait a couple of years until the technology has matured a bit more. The other, is to send a questionnaire as soon as possible, when the technology is still underdeveloped, and gauge the sentiment of a larger population The goal of the questionnaire should be to reach as many auditors as possible and measure their receptibility and opinions on blockchain technology, in both an accounting and auditing setting. By sending a questionnaire to as many as possible, we get a broader understand of what auditors think. One of the limitations of this research was its scope, as it was limited to only nine auditors.

Another future research would be to conduct more interviews, but with IT-auditors working at Big 5 companies. IT auditors are the people who are at the forefront of technology, constantly evaluating alternatives. As we can see in this research, the IT-auditors had more expertise in this area, but they still understood how it could be used to assist financial auditors and clients. By interviewing IT auditors, we would receive a better understanding of whether it would be potentially feasible to use blockchain for accounting and auditing purposes.

7. Summary in Swedish

Bokföring, revision och blockkedja – intervjuer med finländska revisorer om blockkedja

7.1. Inledning

Ordet blockkedja är kanske mest välkänt i sammanhanget med bitcoin och andra kryptovalutor, samt hur deras priser skjutit i höjderna och sedan sjunkit lika snabbt. Det som dock inte ofta talas om är den praktiska användningen som blockkedjor har, vid sidan om bitcoin och kryptovalutor. I vissa kretsar talas det om att blockkedjeteknik kommer att bli den fjärde industriella revolutionen, vilket kommer att förändra hur vissa branscher/sektorer fungerar.

Det här gäller även bokförings- och revisionsbranschen, eftersom Big 5 (KPMG, Deloitte, PwC, BDO och EY) aktivt undersöker hur man kan utnyttja blockedjeteknik. Även nya organisationer har grundats för att undersöka hur man kan integrera blockkedjeteknik i samband med bokföring och revision.

Det finns ett stort intresse för blockkedjor, men väldigt få undersökningar har gjorts om vad revisorerna själva anser om den teknologin som de möjligen kommer att arbeta med i framtiden.

7.2. Syfte

Målet med den här avhandlingen är att undersöka de finska revisorernas mottaglighet för blockkedjeteknik i samband med bokföring och revision. Eftersom revisorer är experter på både bokföring och revision, kommer de att intervjuas gällande möjlig användning av blockkedjeteknik på respektive område. Det är viktigt att höra deras åsikter om den möjliga framtiden för bokföring och revision.

7.3. Teori

Blockkedja grundar sig på trippelbokföring, som i sin enkelhet innebär att det finns tre sidor i bokföringen istället för två sidor som i dubbelbokföring. Precis som dubbelbokföring innehåller trippelbokföring kredit- och debetsidor, men den tredje sidan som är unik för trippelbokföring kallas för kvittot. Kvittot lagrar information om

vem som genomfört en transaktion, till vem den gått och varför. Ännu mera information kan förvaras i kvittot, beroende på vad användaren vill spara. För att kvittot ska fungera, måste det finnas en pålitlig tredje part som bekräftar dessa transaktioner och skriver under dem med sin kryptografiska nyckel. Problemet blir dock då hur man ska försäkra sig om att den tredje parten är pålitlig. För att lösa det här problemet utvecklades blockkedjeteknik.

Blockkedja är en decentraliserad (distribuerad) databas i vilken kopior av samma information lagras i noder (datorer). Informationen som lagras i en blockkedja är krypterad i så kallade block och lagras i en lång kedja som refererar tillbaka till det förra blocket som skapades, vilket ger tekniken namnet blockkedja. Den här konstruktionen gör informationen på blockkedjan oföränderlig och varje förändring som tillåts kan spåras direkt till den som gör det.

Eftersom blockkedjor är decentraliserade, måste det finnas mekanismer som förhindrar manipulation och det här åstadkoms genom olika konsensusmekanismer. Konsensusmekanismen innebär att nätverket på egen hand, utan en central bestämmande kraft, kommer överens om vad som ska lagras på nätverket. Den vanligaste konsensusmekanismen är ”Proof of Work”, eller bevis-på-arbete, som kräver att noderna på nätverket löser kryptografiska pussel för att skapa nästa block, som bekräftar de transaktioner som skett i nätverket. Efter att pusslet är löst, och blocket är skapat, börjar noderna lösa nästa pussel. De noder som hjälper att lösa ett pussel får en belöning, och beroende på hur stor del av pusslet de löst får de en olika stor belöning. Belöningen fungerar även som ett incitament för att få flera människor att delta i blockkedjan, eftersom ju fler deltagare det finns, desto mindre är risken att det sker missbruk av nätverket där någon kunde äga över 51 procent av nätverket, vilket skulle ge den en bestämmande makt över allt som sker i nätverket

7.4. Tidigare Studier

I tidigare studier om blockkedjeteknik i samband med bokföring och revision har det indikerats att konsolideringen av transaktioner för revision skulle vara mera tidseffektivt med blockkedjeteknik, eftersom all data skulle vara digital och tillgängliga direkt på ett och samma nätverk. Bokföringsinformation kan teoretiskt vara betydligt mera pålitlig, eftersom all information som sparas på en blockkedja är

teoretiskt oföränderlig. Strukturen hos blockkedjan skulle även göra det mycket svårt, om inte omöjligt, att förfalska eller manipulera information. Det finns dock fallgropar, eftersom man tekniskt sett kan mata in falsk eller manipulerad information innan informationen når blockkedjan.

Studier som berör revision och blockkedjor påstår att framtida smarta kontrakt som kommer att utvecklas i revisionssyfte, har potential att märkbart hjälpa revisorer att automatisera revision. Blockkedjor kan dessutom hjälpa till att försnabba revisionen, genom att man kan plocka fram väsentlig information snabbare digitalt, än att be kunder söka fram fysiska verifikat. Potentiellt kan man även sköta revision i realtid, eftersom information som matas in i blockkedjan läggs till i realtid, men det skulle kanske/troligtvis kräva stora omställningar för revisorerna, eftersom deras yrke för tillfället koncentrerar sig på att granska det förflutna. Överlag skulle revisorer, enligt vissa studier, vara tvungna att anpassa sig till en totalt digital framtid där det förväntas att de innehar kunskap om programmeringsspråk, samt hur blockkedjor fungerar.

Det som förväntas mest från blockkedjeteknik är att smarta kontrakt skulle lätta på arbetsbördan inom både bokföring och revision. Det finns redan smarta kontrakt implementerade i vissa aktiva blockkedjor, som till exempel Ethereum. Smarta kontrakt är inte ”intelligenta kontrakt”, utan små självständiga datorprogram som utför förhandsbestämda uppgifter när vissa kriterier/omständigheter uppfylls. Ett bra exempel i samband med bokföring, är ett inventariesmartkontrakt som sköter betalningen av varor som kommit till lagret. En arbetstagare matar in på blockkedjan varorna som anlänt till lagret och smart kontraktet betalar automatiskt räkningen då den bekräftat att alla varor anlänt från leverantören. Vid revision kan smartkontrakten ta över och granska enkla transaktioner, medan revisorerna själva granskar de mera komplicerade transaktioner.

Det finns dock vissa nackdelar samt begräsningar med blockkedjor. En av dessa är en så kallad ”majoritetsattacken”, vilket innebär att någon inom blockkedjenätverket äger 51 procent av nätverkets kapacitet. Eftersom den här personen då har bestämmandemakten över nätverket, kan dom teoretiskt ändra på information som redan tidigare matats in på blockkedjan. Situationer som dessa är sällsynta, men

möjliga. En situation där det här kan hända är inom företag där det finns få noder och blockkedjan är centraliserad.

En stor nackdel med publika blockkedjor är att informationen som lagras på dessa är tillgängligt för vem helst. Pseudonymer kan hjälpa till att dölja vem som gör vad, men man kan inte utesluta att någon möjligen kan avslöja vem som ligger bakom en pseudonym.

7.5. Metodologi

Den här undersökningen är en kvalitativ studie, med intervjuer av finska revisorer om blockkedjeteknik i samband med bokföring och revision. Orsaken till att det gjordes en kvalitativ studie är att det undersökta området är nytt. Det finns inga tidigare studier i Finland inom det här området och därför är det här en form av pilotstudie.

Det finns två hypoteser i den här avhandlingen:

1. Blockkedjeteknik och den distribuerade databastekniken kommer att ändra på hur bokföring fungerar
2. Blockkedjeteknik och den distribuerade databastekniken kommer att ändra på hur revision fungerar.

För den här studien har jag intervjuat arbetstagare från Big 5-företagen (KPMG, Deloitte, PwC, BDO och EY). Orsaken till det här är att utomlands har Big 5-dotterföretag undersökt hur blockkedjeteknik kan utnyttjas i samband med bokföring och revision.

I det här fallet beslöt jag att revisorerna som kommer att intervjuas, skulle ha arbetserfarenhet från två år ända upp till fyrtio år. Tanken bakom det här valet, är att få en så bred population som möjligt, med åsikter från revisorer som nyligen inlett sin karriär, sådana som är i mitten av sin karriär och även sådana som är i slutet av sin karriär eller redan har pensionerat sig.

Intervjuerna utfördes både på respondenternas kontor och över telefon och skype.

Totalt var nio revisorer villiga att delta i intervjun. Att så få ville ställa upp för intervju är inte förvånande, eftersom blockkedjeteknik är en relativt ny teknik och därför har

undersökts väldigt lite. I det här fallet fick jag en bra och mångfaldig population att intervjua.

Eftersom blockkedja är en relativt ny teknik, beslöts jag att skicka ut ett introduktionsbrev som gav en kort förklaring av tekniken, ifall de som deltog inte hade förhandskunskaper om blockkedjor före intervjun. Tanken med intervjun var att mäta mottagligheten samt kunskapsnivån hos revisorerna och därför skickades ett förklaringen om tekniken.

Frågorna som ställdes till revisorerna var indelade i fyra olika kategorier:

1. Förhandskunskap om blockkedjeteknik

2. Tankar om den grundläggande teknologin.

3. Tankar om avancerade funktioner och åsikter om bokföringens samt revisionens framtid i relation till blockkedjeteknologi

4. Den sista frågan var en öppen fråga, som gav möjlighet till respondenterna att kommentera fritt.

7.6. Analys av Frågorna

De första två frågorna var, om respondenterna hade hört om blockkedjeteknik före intervjun, och om huruvida företagen där de arbetar hört om blockkedjeteknik eller om har deras kollegor uttryckt intresse för blockkedja.

Sex av de nio intervjuade hade hört om blockkedjeteknik före intervjun. I de flesta fallen hade respondenterna hört om blockkedjor genom diskussioner om virtuella valutor och hur de ska värderas i bokslut. Två av dessa respondenter hade fördjupat sig i blockkedjeteknik och även gått på föreläsningar.

Överlag hade revisorerna inte lagt märke till att deras arbetsgivare uttryckt intresse för blockkedjeteknik, men däremot hade de hört att vissa av deras konsultkollegor och kunder uttryckt intresse.

En av de viktigaste aspekterna hos blockkedjor är oföränderligheten hos informationen, det vill säga om information matats in på blockkedjan, kan man inte

gå tillbaka och ändra på den. När det kommer till bokföring och revision vill man att bokföringsinformationen är pålitlig och därför frågas om blockkedjeteknik kan öka pålitligheten av bokföringsinformationen. I det här fallet var det tudelat. Fyra personer ansåg att det kommer att öka pålitligheten, eftersom informationen på blockkedjenätverket inte går att manipulera i efterhand. Dessutom skulle informationen bli mera pålitlig om den skulle matas in i nätverket av maskiner. De som ansåg att det inte ökar på pålitligheten, konstaterade att informationen kunde manipuleras förrän den sätts in på blockkedjan. Fastän blockkedjor erbjuder oföränderlig information, betyder det inte att den inmatade informationen är 100 procent korrekt.

Blockkedjeteknik eliminerar de mänskliga mellanhänderna som kunde ha en negativ inverkan på förtroende för informationen och därmed borde den information som existerar på en blockkedja teoretiskt vara mera trovärd. Det finns inte en centralt bestämmande enhet, utan alla deltagare på nätet når ett gemensamt beslut om att den information som matats in på en blockkedja kan betraktas som pålitlig. Respondenterna ansåg att elimineringen av mellanhänderna på en blockkedja kan öka trovärdigheten av den information som finns på den. Eftersom informationen är oföränderlig, kan man med stor sannolikhet anta att informationen också är trovärdig. Respondenterna medgav att information som matas in dock kan vara felaktig och man måste kontrollera manuellt att bokningar är korrekta.

Som tidigare nämnts kan en blockkedja antingen vara en privat eller öppen blockkedja. Dessa två former är de mest populära, men skiljer sig stort på hur de fungerar. Tekniskt sett är öppna blockkedjor säkrare eftersom noderna i nätverket inte är centraliserade, men alla som vill har åtkomst till informationen har det. Privata blockkedjor däremot kan skydda informationen bättre och endast ge tillgång åt bekräftade användare, men risken för 51 procents attacker ökar märkbart eftersom noderna är centraliserade. Med tanke på dessa skillnader är det viktigt att veta vad revisorerna tror att företag kommer att använda. Alla respondenter svarade att privata kommer att användas mest, helt enkelt för att de skulle kunna skydda vem som har tillgång till deras information. En respondent föreslog att man eventuellt kunde förflytta sig till en blockkedja, som administreras av ett konsortium, där flera företag delar på noder, för att minska på riskerna.

En av de mest intressanta funktionerna med blockkedjor, är att den erbjuder uppföljning av information i realtid. Teoretiskt kunde det här även användas av revisorer för att utföra revision i realtid. De flesta av respondenterna ansåg att det kunde vara en bra idé. Man skulle inte behöva vänta på att få information, utan man kunde ta och direkt plocka ut det som man finner väsentligt. Det här skulle också ändra på yrket i sin helhet. Vissa ansåg att realtid inte kommer att vara nödvändigt och att revision alltid kommer att titta på det förflutna. Överlag skulle det finnas för mycket oväsentlig information i en realtids revision.

Det här leder oss in på digital eller digitaliserad information, vilket blockkedjor består av. All information på blockkedjenätverket är digitaliserat och tillgängligt från vilken nod som helst på nätverket. Genom det här kan man alltid nå informationen, oberoende var man är, så länge man kan nå en nod. Respondenterna ansåg att idén är bra, men många påpekade att det finns liknande lösningar redan nu hos stora företag. Däremot kan det vara till en stor fördel om det integreras i företagets hela system. Vissa spekulerar att man i framtiden inte behöver åka på kundbesök, utan istället kan man få all information man behöver direkt till ens arbetsstation.

De smarta kontrakten som nämndes tidigare, spelar även en stor roll i en möjlig framtid där blockkedjeteknik används av revisorer. Tidigare studier gjorda på det här området har påpekat att de smarta kontrakten kan förändra yrket märkbart. Till exempel kan smarta kontrakt för bokföring självständigt sköta enkla bokningar, medan bokförare övervakar processen. Det samma gäller även för revision, de smarta kontrakten kontrollerar enkla bokningar, medan revisorerna tar hand om mera komplicerade transaktioner. När revisorerna frågades om de anser att smarta kontrakt för bokföring är en bra idé, ansåg de flesta att det är det. De kan lätta på arbetsbördan, samt förhoppningsvis göra informationen mera pålitligt och se till att det uppstår färre fel. Dock ansåg dom att man inte kan förlita sig blint på smarta kontrakt, eftersom det möjligen kan uppstå fel.

De smarta kontrakten för revision kommer enligt respondenterna att hjälpa till att minska på arbetsbördan. Det finns dessutom möjligheten att skräddarsy smarta kontrakten då olika företag redovisas, vilket kommer att ge flexibilitet i områden där det inte ännu finns det. Det finns dock en fara att revisorerna kan förlita sig för

mycket på vad de smarta kontrakten säger, istället för att analysera vad som egentligen sker.

Trodde revisorerna däremot att blockkedjeteknik kommer att leda till förändringar i deras arbetsuppgifter, ifall blockkedjeteknik tas i bruk i deras företag? Majoriteten av respondenterna ansåg att det kommer att ske. Vissa ansåg att jobbet kommer att bli mera tekniskt betonat, och mera fokus kommer att läggas på data-analys. Därutöver måste revisorer också lära sig att läsa kod, samt även möjligen programmera. Eventuellt kan det här leda till att nya revisorsroller uppkommer, som till exempel exklusivt granskar smart kontrakt och blockkedjor. De som inte ansåg att det kommer att förändras, sa att revisorns roll är att granska det förflutna och teknologin kommer inte att ändra på den här rollen.

Blockkedja är en ny teknik som inte ännu har testats i bokförings- och revisionssammanhang och därför är det viktigt att fastställa om revisorerna ser några svagheter i teknologin. De flesta respondenterna ansåg att det finns svagheter, vilket beror på att man inte kan vara absolut säker på att informationen som matats in på blockkedjor är korrekt. I så fall borde man ge total kontroll över blockkedjor till maskiner och inte låta en människa röra det.

Den sista frågan var om revisorerna om teknologin gav upphov till andra kommentarer, som de inte kunnat uttrycka under intervjun. De som hade extra synpunkter ansåg att det är en intressant utveckling och att det blir spännande om teknologin bryter igenom. Överlag tror de att revision kommer att bli mera datadrivet. Dessutom kommer det att krävas en hel del tekniskt kunnande för att kunna genomföra revision i framtiden. Teknologin kommer att eventuellt att tas i bruk, men de konservativa industrierna kommer att ta tid på sig att implementera det.

7.7. Slutsatser

Målet med den här avhandlingen var att ta reda på hur mottagliga de finska revisorerna skulle vara för blockkedjeteknik, för både bokföring och revision. Det har inte tidigare gjorts liknande studier om det här ämnet i Finland. Många av de stora internationella bokförings- och revisionsföretagen har visat intresse för blockkedjeteknik och det har gjorts akademiska studier om hur teknologin kunde tillämpas inom både bokföring och revision. Problemet har dock varit att man inte

intervjuat revisorer, som möjligtvis kommer att arbeta med den här tekniken, om den tas i bruk. Det är detta problem den här avhandlingen försökt lösa genom att intervjua revisorer i Finland.

I regel verkar det som om revisorerna i Finland har ett intresse och är mottagliga för blockkedjeteknik. Diskussionerna som fördes med revisorerna visade att dom väldigt snabbt kunde uppfatta hur teknologin fungerar, samt hur den skulle fungera i en revisions- eller bokföringssituation.

På basis av de första frågorna verkar det som att blockkedjeteknik inte har diskuterats väldigt mycket bland revisorer, vilket är förståeligt, för tekniken är ny och revisorer brukar inte analysera den teknologin som stöder deras arbete, eller hur de olika programmen de använder fungerar.

Även trots intervjun innehöll många frågor som rörde sig kring tekniska lösningar, vilket blockkedjetekniken erbjuder, lyckades revisorerna diskutera ämnet på en teoretisk nivå. Till exempel var diskussionerna kring oföränderlighet intressanta, där revisorerna ansåg att det kunde positivt påverka trovärdigheten av bokföringsinformation, men inte pålitligheten av den.

Om blockkedjeteknik kommer att slå igenom, är det sannolikt att det är de smarta kontrakten som revisorerna kommer att använda mest. De diskussioner som fördes kring ämnet, antydde att revisorerna ser stora fördelar med hur de kan automatisera olika områden inom revision och bokföring, samt göra granskningarna effektivare och snabbare.

Genom att knyta undersökningen tillbaka till de tidigare akademiska studierna gjorda om blockkedjeteknik och teoretisk användning av blockkedjeteknik inom bokföring och revision, kan vi se att det skulle vara viktigt för revisorerna att få vara med att utveckla hur teknologin kommer att användas i framtiden. Deltagarna i intervjuerna hade många bra åsikter och frågor om teknologin och visade ett klart intresse i framtida applikationer av den.

Om blockkedjor kommer att användas i framtiden kommer det att ändra på revisionsyrket, vilket de flesta revisorerna medgav. Men, hur yrket kommer att

ändras är det ännu för tidigt att säga. Överlag verkar det redan nu som att revisionsyrket blir mera it-kunskapskrävande ansåg vissa av de intervjuade.

Det är för tidigt att säga om blockkedjor kommer att slå igenom som ett verktyg som kommer att användas inom bokföring och revision, men om det sker verkar det som att de finska revisorerna är klara att ta emot nyheten och lära sig hur det fungerar praktiskt, inte endast teoretiskt.

Word List

Blockchain: A public/private digital ledger, that is decentralized and distributed across a network of computers to prevent real-time and retroactive manipulation of records. Runs independently and does not require a third-party/human to confirm transactions occurring on the network.

Consensus algorithm: An algorithm used by the blockchain network to reach an agreement on whether the values about to be entered onto the blockchain are indeed valid.

PoW: Proof of Work is a consensus algorithm used by multiple blockchains to confirm the validity of transactions occurring on the network. Computers participating on the network solve mathematical puzzles through a process called “mining”. The more computer participates on the network, the harder the puzzle becomes to solve, and more computational power will be required to solve the problem. Once the puzzle is solved, the transactions that happened in-between the last puzzle was solved and this puzzle was solved, will be verified and added to the ever-growing list of blocks on the blockchain. Those who participated in the “mining” of the block receive freshly minted currency that the PoW blockchain uses, as a reward. The more computational power a “miner” gives to the network, the larger the reward. Mining works as a method to prevent DoS attacks and spamming.

PoS: Proof of Stake is a method wherein instead of using computers to conduct calculations, the participants on the network “stake” the tokens they own, for the chance to be selected to verify the transactions happening on the network. The more a participant stakes on the network, the higher the chance of being selected to verify the transactions. Those who partake in the validation of the blocks will receive a reward, in the form of the transaction fees that people paid to send payments on the PoS network.

Hashrate: The amount of processing power the blockchain network has available to conduct the “mining”.

Public blockchain: A blockchain that can be joined by anyone. Everyone on the blockchain network can read, write and participate. Also known as a permissionless blockchain.

Private blockchain: A blockchain that only can be joined if one has been given permission. Central authority gives access to read, write and participation functions. Also known as a permissioned blockchain.

Consortium blockchain: A blockchain that is a hybrid of public and private blockchain. Companies are first allowed onto the network, after which they can read, write and participate in the blockchain. They can technically see what other companies enter onto the blockchain, but transactions might be encrypted to prevent this. Also known as a federated blockchain.

Smart contract: A small computer program that carries out tasks when certain pre-determined conditions are met, e.g. Releasing payments when all bought products have been received.

Cryptocurrency: Is a virtual or digital peer-to-peer currency, that has been secured by encryption.

References

ABC.Accounting blockchain coalition. Retrieved from https://accountingblockchain.net/

ACFE. (2019). Report to the nations - 2018. Retrieved from https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

AICPA. (2017). Blockchain technology and its potential impact on the audit and assurance profession. Retrieved from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf

Alibaba Cloud. (2018). World's first blockchain-based cross-border remittance service by ant financial. Retrieved from https://www.alibabacloud.com/blog/worlds-first-blockchain-based-cross-border-remittance-service-by-ant-financial_594030

Alrawi, H. A., & Ambashe, M. (2018). The development of accounting through the history. *Ijame,*

Appelbaum, D., & Nehmer, R. (2017). Designing and auditing accounting systems based on blockchain and distributed ledger principles. *Feliciano School of Business,*

Balanc3. (2017). Announcing Balanc3: Quickbooks for token launches. Retrieved from https://media.consensys.net/announcing-balanc3-quickbooks-for-token-sales-9e54cb00df66

Baran, P. (1964). On distributed communications networks. *IEEE Transactions on Communications Systems, 12*(1), 1-9.

Bryman, A., & Bell, E. (2015). *Business research methods* (Fourth edition ed.). Oxford: Oxford University Press, UK. Retrieved from https://ebookcentral.proquest.com/lib/[SITE_ID]/detail.action?docID=4776950

Buterin, V. (2013). A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM. Retrieved from https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Carlin, T. (2018). Blockchain and the journey beyond double entry. *Australian Accounting Review,* doi:10.1111/auar.12273

Cîndea, M., Cîndea, I. M., Ciurariu, G., Trifu, A., & Durdureanu, C. (2011). History of accountancy. A chronological approach. *IPEDR Proceedings, 11*, 18-24.

CNBC. (2019). Swift CEO announces tie-up with blockchain start-up R3. Retrieved from https://www.cnbc.com/2019/01/30/swift-announces-tie-up-with-blockchain-firm-r3-at-paris-fintech-forum.html

Coyne, J. G., & McMickle, P. L. (2017). Can blockchains serve an accounting purpose? *Journal of Emerging Technologies in Accounting, 14*(2), 101-111. doi:10.2308/jeta-51910

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems, 31*(3), 5-21. doi:10.2308/isys-51804

Deery, B., Lu, J., Johnston, D. & Kirby, P. (2018). Factom: Business processes secured by immutable audit trails on the blockchain. Retrieved from https://www.factom.com/assets/docs/Factom_Whitepaper_v1.2.pdf

Deloitte. (2016). *Blockchain: A game changer in accounting.* (). Retrieved from https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf

Deloitte. (2018). Blockchain: Opportunities for health care
A new model for health information exchanges. Retrieved from https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html

EY. (2016). *Chain reaction: How blockchain technology could revolutionize the finance function.* (). Retrieved from https://www.ey.com/Publication/vwLUAssets/EY-chain-reaction/$FILE/EY-chain-reaction-how-blockchain-technology-could-revolutionize-the-finance-function.pdf

EY. (2017). The risks and opportunities of blockchain
disruption in the boardroom. Retrieved from

https://www.ey.com/gl/en/issues/governance-and-reporting/center-for-board-matters/ey-the-risks-and-opportunities-of-blockchain

EY. (2018a). Blockchain has the potential to streamline and accelerate business processes and reduce risk. Retrieved from https://www.ey.com/en_gl/blockchain

EY. (2018b). IFRS (#) accounting for crypto-assets. Retrieved from https://www.ey.com/Publication/vwLUAssets/EY-IFRS-Accounting-for-crypto-assets/$File/EY-IFRS-Accounting-for-crypto-assets.pdf

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2018). *A survey on privacy protection in blockchain system* doi://doi.org/10.1016/j.jnca.2018.10.020

Gabison, G.*Policy considerations for the blockchain technology public and private applications*

Gramoli, V. (2017). *From blockchain consensus back to byzantine consensus* doi://doi.org/10.1016/j.future.2017.09.023

Grigg, I. (2005). Triple entry accounting. *Systemics Inc,*

Ian Grigg. (2005). Triple entry accounting. Retrieved from http://www.dx.doi.org/10.13140/RG.2.2.12032.43524

IBM. (2018a). Maersk and IBM introduce TradeLens blockchain shipping solution. Retrieved from https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution

IBM. (2018b). We.trade. Retrieved from https://www.ibm.com/case-studies/wetrade-blockchain-fintech-trade-finance

Kiviat, T. I. (2015). Beyond bitcoin: Issues in regulating blockchain tranactions. *Duke LJ, 65*, 569.

Kokina, J., Mancha, R., & Pachamanova, D. (2017). Blockchain: Emergent industry adoption and implications for accounting. *Journal of Emerging Technologies in Accounting, 14*(2), 91-100. doi:10.2308/jeta-51911

Kozlowski, S. (2018). An audit ecosystem to support blockchain-based accounting and assurance. *Continuous auditing* (pp. 299-313) Emerald Publishing Limited. doi:10.1108/978-1-78743-413-420181015 Retrieved from http://www.emeraldinsight.com/10.1108/978-1-78743-413-420181015

KPMG. (2016). KPMG, InTech and fundsquare launch blockchain-based product for asset managers. Retrieved from https://home.kpmg/lu/en/home/media/press-releases/2016/12/kpmg-intech-fundsquare-launch-blockchain-based-product.html

KPMG. (2018a). Audit point of view
the blockchain shift will be seismic. Retrieved from https://assets.kpmg/content/dam/kpmg/ca/pdf/2018/02/apov-blockchain-feb-2018.pdf

KPMG. (2018b). Blockchain and the future of finance. Retrieved from https://advisory.kpmg.us/content/dam/advisory/en/pdfs/blockchain-future-finance.pdf

Lai, R., & LEE Kuo Chuen, D. (2018). In Lee Kuo Chuen D., Deng R.(Eds.), *Chapter 7 - blockchain – from public to private* Academic Press. doi://doi.org/10.1016/B978-0-12-812282-2.00007-3

Lampard, R., & Pole, C. (2015). *Practical social investigation: Qualitative and quantitative methods in social research* Routledge.

Linux Foundation. (2018). What is hyperledger fabric? Retrieved from https://hyperledger-fabric.readthedocs.io/en/release-1.3/blockchain.html

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

O'Leary, D. E. (2017). Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems. *Intelligent Systems in Accounting, Finance and Management, 24*(4), 138-147. doi:10.1002/isaf.1417

PwC. (2018). PwC france et afrique francophone s'associe à la fondation request network afin de renforcer son expertise sur la blockchain Retrieved from https://www.pwc.fr/fr/espace-presse/communiques-de-presse/2018/juillet/pwc-france-afrique-francophone-s-associe-a-la-fondation-request-network.html

Request Network. (2018). Request network the future of commerce a decentralized network for payment requests. Retrieved from https://request.network/assets/pdf/request_whitepaper.pdf

Rozario, A. M., & Vasarhelyi, M. A. (2018). Auditing with smart contracts. *The International Journal of Digital Accounting Research, 18*, 1-27. doi:10.4192/1577-8517-v18_1

Rückeshäuser, N. (2017). Do we really want blockchain-based accounting? decentralized consensus as enabler of management override of internal controls.

Santander Bank. (2018). Santander becomes first UK bank to introduce blockchain technology for international payments with the launch of a new app Retrieved from https://www.santander.com/csgs/Satellite?appID=santander.wc.CFWCSancomQP01&c=GSNoticia&canal=CSCORP&cid=1278712674240&empr=CFWCSancomQP01&leng=en_GB&pagename=CFWCSancomQP01%2FGSNoticia%2FCFQP01_GSNoticiaDetalleMultimedia_PT18

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., . . . Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity, 52*(4), 1893-1907. doi:10.1007/s11135-017-0574-8

Simoyama, F. D. O., Grigg, I., Bueno, R. L. P., & Oliveira, L. C. D. (2017). Triple entry ledgers with blockchain for auditing. *International Journal of Auditing Technology, 3*(3), 163-183.

Szabo, N. (1994). Smart contracts. Retrieved from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Truby, J. (2018). Decarbonizing bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies. *Energy Research & Social Science, 44* doi:10.1016/j.erss.2018.06.009

Walle, A. H. (2015). *Qualitative research in business: A practical overview*. GB: Cambridge Scholars Publishing. Retrieved from http://lib.myilibrary.com?ID=804202

Yu, T., Lin, Z., & Tang, Q. (2018). *Blockchain: Introduction and application in financial accounting* doi:10.2139/ssrn.3258504

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352-375.

Appendix A

Interview guide:

Previous knowledge of blockchain

Question 1. Have you heard about blockchain before this interview?

- Where have you heard about blockchain?

Question 2. Has your company or colleagues expressed interest in blockchain?

- In what context or who has expressed interest?

Fundamentals of blockchain

Question 3. Will immutability increase reliability of accounting information?

- If yes, why?
- If no, why not?

Question 4. Will immutability increase trust of accounting information?

- If yes, why?
- If no, why not?

Question 5. Would corporations prefer private or public blockchains?

- Why would they prefer the alternative you chose?

Enhanced capabilities provided by blockchain

Question 6. Would information in real-time would be useful for auditors?

- Why would it be beneficial?
- Why would it not be beneficial

Question 7. Can digitized/distributed information from the blockchain ease auditing work?

Question 8. Are accounting smart contracts a good idea?

Question 9. Are auditing smart contracts a good idea?

Future of the auditing career due to blockchain

Question 10. If blockchain were to be implemented, will it change the auditing job?

Question 11. Do you perceive some fundamental weaknesses in blockchain?

- If yes, what is that you see?

Question 12. Do you have any other comments?

Appendix B

Introduction letter:

Hi, my name is Niclas Gröndahl and I'm a master's student enrolled at Åbo Akademi.

The subject I am researching for my master's thesis is "The potential future of auditing: Auditors opinions on the impact of blockchain in accounting and auditing".

This accompanying letter has the purpose of explaining in basic terms what blockchain is and giving some thoughts on what will be discussed during the interview.

The goal:

The goal of the interview is to gauge the knowledge, opinions and expectations of both current and former auditors in Finland, in relation to blockchain in their jobs and the future of accounting and auditing.

Among different topics that will be discussed and explored are; the reliability and trust of information on a distributed network, digitalization of all material, immutability of information, benefits of the same information being distributed to everyone, will companies be willing to participate in open blockchains or will they keep themselves to private blockchains, the automation of certain aspects through self-executing programs, will accounting and auditing change together with regulation to support blockchain, how will the job of an auditor change, and more.

The interview will take approximately 20-40 minutes depending on the amount of discussion.

The next partis intended to be a refresher for those who know about blockchain and a short introduction on the basic concepts of blockchain for those who are new to it.

A short explanation on what blockchain is:

Blockchain is the technology empowering cryptocurrencies like Bitcoin and Ethereum. In its basic essence, a blockchain is a decentralized database (also known as a digital ledger), which has the same data distributed over all the participating computers (so called nodes) on the network. Everyone always has the same data available.

When data is entered on the blockchain, all participants (nodes) on the network need to reach "consensus". Consensus means agreeing that the transaction or event took place, and is an automated process, where no human interaction is needed. When consensus cannot be reached, it is not entered onto the blockchain, and rejected. There exist several different ways of reaching consensus, some are based on solving mathematical puzzles (proof of work), others are based on the amount of stake that someone holds in the network (proof of stake). All consensus methods have the purpose of verifying that the data being entered onto the blockchain is legitimate.

This makes blockchains "trustless" there is no intermediary or third party overseeing the traffic, every participant has the same rights and power, no single person or entity is in control. Everything is solved on the network.

The data entered on the blockchain is immutable, which means that once it is on there, it cannot be changed, this is by design. This record is now cryptographically sealed to prevent tampering. Blockchains are append only, so if any changes need to be done, the data needs to be corrected by adding or subtracting in the future. All changes are signed by a personal “cryptographic” key. Therefore, everything that is entered leaves a trace that it is impossible to remove and/or fake.

The integrity of the data is ensured by a cryptographic hash that is generated, which is calculated from the content that is inside of a “block”. The block is a collection of the data bundled together, that is being entered onto a blockchain. The hash works as a fingerprint for a block, which proves that none of the data in that specific block has been changed after it came into existence. Every block links to the previous blocks hash, which in turn links to that previous blocks hash and forth. This creates a chain, of hashes which prove no data has been tampered with. This is where the name blockchain comes from.

Blocks are uploaded with a time-delay onto a blockchain, and the speed entirely depends on the design of the blockchain. This can allow for near real-time dissemination of information that is being entered onto a blockchain.

If tampering did occur on a blockchain, the hash for that block would change and the chain would break, since there would be no corresponding hashes. Tampering would be noticed very quickly. However, manipulation of the blockchain can be done by gaining 51% of the network capacity, with something known as a “majority attack”, although very unlikely. Conducting a 51% attack is very resource intensive. Some blockchains are more resistant and some less resistant to these kinds of attacks.

Any and all data can be tokenized on a blockchain. Some companies are tokenizing property rights, supply chains and more. Currencies can also be tokenized to give a digital representation of currencies used in the real world.

Blockchains come in many shapes and sizes, but they are normally divided into three parts: public, private and consortium. Public blockchains are open to anyone, to both append data to as well as view. Private blockchains are only accessible by pre-vetted participants, these are also sometimes called permissioned blockchains. Consortium blockchains are blockchains that are run by an organization which allows for other organizations to participate in the usage. These are sometimes even known as corporate blockchains.

Some blockchains support “smart contracts”, which are self-executing computer programs. They self-execute when a certain criteria or threshold has been met. An often-used example is when a product has been received by a company and the smart contract is informed of this, and then releases the payment to the producer who had their goods delivered. Smart contracts are meant to automate different simple processes, with simple logic and/or criteria.

Additional resources:

Below is a link to more resources on how a blockchain works:

http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

If you have any questions, do not hesitate to contact me.

Best regards,

Niclas Gröndahl