How smart contracts can change the insurance industry

- Benefits and challenges of using Blockchain technology
Master Thesis in Informatics

Title: How smart contracts can change the insurance industry
Authors: Habil Kantur and Charles Bamuleseyo
Tutor: Osama Mansour
Date: 2018-05-21

Key terms: Smart Contracts, Blockchain, Insurance, Contract Theory, Opportunities, Challenges, Legal Contracts, Insurance industry, Insurance companies

Abstract
The world is becoming more and more digitized. Recently many industries have started to research the blockchain technology and particularly smart contracts. One industry that so far has not adopted new technology in the same pace as other industries, is the insurance industry so this interview study aims at finding opportunities and challenges for insurance companies that want to learn about smart contracts and its use cases.

By doing a literature review and performing interviews with blockchain experts and insurance company employees, this study found that both IT companies working with smart contracts and the insurance companies have limited knowledge of the legal aspect of smart contracts. The lack of standards and regulations allows IT companies to freely create smart contracts without much quality control. The insurance companies must innovate themselves in order to avoid disruption. The blockchain technology will offer many new insurance types and if the insurance industry fails to adopt the blockchain technology they may face market disruption.

There is much room for future research following this study. It would be beneficial to research how contract theory could be used in practice during the creation of legally binding smart contracts. Furthermore, research around fraud prevention in smart contracts would be interesting as would an in-depth exploration of the ecosystem of third party software and services around smart contracts.
Table of Contents

1. Introduction ............................................................................................................. 1
   1.1. Research gap........................................................................................................ 2
   1.2. Purpose ................................................................................................................ 4
   1.3. Research questions ............................................................................................. 4
   1.4. Delimitation ......................................................................................................... 4
   1.5. Definitions .......................................................................................................... 5

2. Literature Review ..................................................................................................... 8
   2.1. Blockchain .......................................................................................................... 8
   2.2. Public and Private blockchains .......................................................................... 12
   2.3. Benefits of blockchain ....................................................................................... 12
   2.4. Challenges and limitations of blockchain ........................................................... 15
   2.5. Smart contracts ................................................................................................... 17
   2.6. The difficulties of smart contracts ...................................................................... 18
   2.7. Smart contract blockchain platforms ................................................................... 19
       2.7.1. Ethereum ...................................................................................................... 19
       2.7.2. Hyperledger Fabric .................................................................................... 20
       2.7.3. Corda .......................................................................................................... 20
   2.8. Oracles ................................................................................................................ 20
   2.9. DAOs /DACs ..................................................................................................... 22
   2.10. Use cases of blockchain in the insurance industry ............................................ 22
   2.11. Insurance brokers and Agents ......................................................................... 23

3. Theoretical framework ............................................................................................ 24
   3.1. Contract theory .................................................................................................. 25
   3.2. Smart contracts and contract law ...................................................................... 28

4. Research methods .................................................................................................. 31
   4.1. Research approach ............................................................................................. 31
   4.2. Research setting ................................................................................................. 32
   4.3. Methods of data collection ............................................................................... 32
       4.3.1. Secondary data collection ........................................................................... 32
       4.3.2. Sampling techniques .................................................................................. 33
4.3.3. Interviews ................................................................. 35
4.3.4. Questionnaire .......................................................... 37
4.4. Data Analysis .............................................................. 38
4.5. Research credibility ....................................................... 40
4.6. Generalizability ............................................................ 41
4.7. Research ethics ............................................................. 41

5. Results ............................................................................. 42
5.1. Interviews ....................................................................... 42
5.1.1. Third parties ............................................................. 42
5.1.2. Blockchain technology and IT systems ......................... 44
5.1.3. Insurance industry business model ............................... 45
5.1.4. Customer service ....................................................... 46
5.1.5. Regulations .................................................................. 47
5.2. Questionnaire ............................................................... 50
5.2.1. Mutual assent ............................................................ 51
5.2.2. Adequate consideration .............................................. 51
5.2.3. Capacity ..................................................................... 52
5.2.4. Legality ..................................................................... 52
5.2.5. Contract cancellation .................................................. 53
5.2.6. Breaches .................................................................... 54
5.2.7. Renegotiation ............................................................ 55
5.2.8. Smart contract platform .............................................. 55
5.2.9. Blockchain limitations ............................................... 55
5.2.10. Opportunities .......................................................... 56
5.2.11. Challenges ............................................................... 57

6. Analysis .............................................................................. 58
6.1. Blockchain technology in the insurance industry ............... 58
6.2. The law and smart contracts .......................................... 60
6.3. Contract theory ............................................................. 62
6.4. Opportunities ............................................................... 65
6.5. Challenges ................................................................. 71
7. Conclusion .............................................................................................................. 74
7.1. Limitations ........................................................................................................ 75
8. Discussion ............................................................................................................. 77
  8.1. Results discussion .............................................................................................. 77
  8.2. Methods discussion .......................................................................................... 78
  8.3. Implications for research ............................................................................... 79
  8.4. Implications for practice ............................................................................... 80
  8.5. Future research ............................................................................................... 82
9. Reference list ........................................................................................................ 84
10. Appendix A - Interview guide ................................................................. 91
    Appendix B – Questionnaire questions .............................................................. 95
    Appendix C – Categories from the interview transcripts ............................... 97
    Appendix D – Transcripts .............................................................................. 100
List of figures

Figure 1: Decentralized blockchain.................................................................9
Figure 2: Simplified model of a block in a blockchain.................................10
Figure 3: Oracles communicate with different sources.............................21
Figure 4: The four elements of a valid legal contract.................................26
Figure 5: Smart contracts are only legal contracts in some cases..............28

List of tables

Table 1: Generations of blockchain.................................................................12
Table 2: More defenses to contract enforcement........................................25
Table 3: Used search phrases........................................................................33
Table 4: Summary of the interviews...............................................................37
Table 5: Formulation of themes from Interview transcripts.......................39
Table 6: Theoretical framework themes.......................................................50
Table 7: Theoretical framework themes.......................................................50
1. **Introduction**

This chapter introduces the background of Blockchain, smart contracts and the insurance industry and how the technology has developed the past three decades. The knowledge gap, purpose and research questions are specified and the chapter ends with the delimitation of the study as well as definitions used throughout the paper.

**Blockchain and smart contracts**

The world is becoming more and more digitized. Most companies use computers in their everyday work and more and more people use their smart phones to do work on. One industry that so far has not adopted new technology in the same pace as other industries, is the insurance industry. The reason for this could be because of internal struggles over resources and career advancement within management (Knights & Murray, 1992). This is about to change though. In 2016 the Blockchain Insurance Industry Initiative (B3i) was formed as a collaboration between insurers and reinsurers to find out how Distributed Ledger Technologies (DLT) could benefit all the different stakeholders in the value chain (B3i, 2017). For instance, blockchain technology can offer more than just a way to create digital currencies (Nofer, Gomber, Hinz & Shiereck, 2016). Furthermore, it can be used as a replacement for the intermediate trust such as banks or governments because security is built-in. Instead of allowing banks or other institutions to act as guarantee, trust can be used by the blockchain technology and allow digital contracts to form (Alcazar, 2017).

In 1997 the cryptographer Nick Szabo introduced the concept of smart contracts which in short, allows a user to trigger the terms of a digital contract using a user interface (Szabo, 1997). Smart contracts are self-executing snippets of code stored in the blockchain. The code can contain certificates, personal data, licenses or wills for example. These smart contracts can be used in all industries but the banking and in insurance industries are those most likely to be disrupted in the next decade. Since the blockchain is public,
decentralized and distributed it is easy to access it and at the same time offer a secure way of information storage (Cuccuru, 2017).

Morabito (2017) asserts that the major challenges experienced in the insurance today, include falsified claims, labor intensive processes, fragmented data sources and legacy underwriting models. These lead to low customer satisfaction. Creating policies as smart contracts on the blockchain can offer control, precision and traceability for each claim and could lead to automatic payouts.

There are however risks and insecurities with moving contracts to the blockchain. The technology its self is young and not tested on a global scale. For a technology to be used globally it must be both secure and fast. Today blockchains transactions can have high latencies which is a big problem. All the potentially new benefits come at a cost though. Public blockchains will allow anyone to access information on completed transactions at some level. The technology for using smart contracts must be able to keep a certain level of privacy (Benton & Radziwill, 2017).

The study by KPMG International (2017), states that one of the more disruptive applications of blockchain is the development of ‘smart contract’ models. Claims data is shared across all counterparties. Identities and contract provisions are immediately verified thus leading to automatic payments. Furthermore, less adjudication and negotiation required thus reducing costs. From a customer point of view, the handling of an insurance claim will be faster and more automated. From the aspect of an insurance company, the usage of blockchain technology will decrease fraud rate and lower the number of participants involved in claiming processing thus reducing the costs (Nath, 2016).

1.1. Research gap

‘Smart contracts’ is a fairly new phenomenon and there is not much information about smart contracts in the insurance industry. Smart contracts have huge potential in
automating digital processes but since the technology is young it has both conceptual issues as well as practical ones.

The conceptual issues are the different definitions of smart contracts. There are discussions whether smart contracts are legal contracts or not (Giancaspro, 2017; Werbach & Cornell, 2017; Norton Rose Fulbright, 2016). This study tries to make the definition of smart contracts more clear. The practical issues are first, the digital infrastructure and second, the ecosystem of systems needed by smart contracts to work properly.

This study aims to explore what smart contracts are and how they can be facilitated by the insurance industry. The research gap we have identified is the practical use of smart contracts in the insurance industry, both when its considered to be a legal contract and when it is not. Most of the studies conducted by various authors such as; KPMG international (2017), Deloitte (2016), McKinsey&Company (2016), Hans, Zuber, Rizk and Steinmetz (2017), explore the opportunities and challenges of using blockchain technology and smart contracts in the insurance industry but do not explain the legal perspective of smart contracts. Few studies discuss the opportunities and challenges of using blockchain technology and smart contracts in the insurance industry as well as presenting an in-depth analysis of the legal perspective of smart contracts. The term smart contract is often mistaken to be a legal contract. In reality, smart contracts deal with protocols that trigger automatic execution of contractual terms and conditions set by parties and stored in the blockchain (PWC, 2017). This raises a question whether smart contracts are legally valid.

The study tries to explain how and why the insurance industry needs to adopt this technology and adapt the business models accordingly. It also explains the legal perspective of smart contracts.
1.2. Purpose

The purpose of this study is to understand how insurance companies can adapt to the changes that smart contracts might bring.

1.3. Research questions

What are the opportunities and challenges for the insurance industry using smart contracts?
What difference can the blockchain technology make to the insurance industry?

1.4. Delimitation

This study focused on how smart contracts could change the way in which the insurance industry does business, particularly the auto and life insurance parts of the industry. Other types of insurances were not looked into.

Ethereum as described in this study concentrates on its general functionality and its specific uses for smart contracts. Other properties or uses of Ethereum, such as financial derivatives or its use as a currency is beyond the scope of this study.

This study will only mention the usefulness of smart contracts in coordination with the Internet of Things, Artificial Intelligence and Big Data in the section of discussion and will not explain the necessary technological ecosystem in more in detail.

The security issues were deliberately more or less left out of this study because this aspect of the studied topic has a big enough impact to have its own study.

Contract theory has a history of different opinions on what should be part of the theoretical framework. This study uses only a simplistic model of contract theory that can be applied to smart contracts and will not discuss the roadmap of events that has shaped contract theory into what it is today.
The effects of the General Data Protection Regulation (GDPR) on the blockchain technology is out of the scope of this study.

1.5. Definitions

AI – Artificial Intelligence

API – Application Programming Interface

Big Data – “is high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.” (Gartner IT Glossary, n.d.)

Bitcoin – a cryptocurrency created by Satoshi Nakamoto (Nakamoto, 2008)

Blockchain – “a distributed database and shared ledger that maintains continuous growing list of records (blocks) in a chronological order” (The Institutes, 2017)

Consensus protocol –“is a computer protocol in the form of an algorithm constituting a set of rules for how each participant in a blockchain should process messages and how those participants should accept the processing done by other participants” (Smart Contracts Alliance, 2016).

Cryptocurrency – “a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of currency” (Greenberg, 2011).

Cryptography – “the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication” (Menezes, Van Oorschot & Vanstone, 1996, p. 4)
DAO – Decentralized Autonomous Organization. A virtual entity on the blockchain consisting of members that have the right to spend the funds contained within the entity or modify the code that makes up the entity and its functionalities (Buterin, 2014).

Distributed Ledger Technology (DLT) – “Distributed ledgers are a type of database that is spread across multiple sites, countries or institutions, and are typically public copies of each other. Records are stored in transactions located in blocks, one after the other in a continuous ledger, but they can only be added when the participants reach a quorum” (Walport, 2016, pp. 17–18)

Ethereum – A blockchain platform that allows different protocols to be merged together and improve its functionalities using programming and thus creating consensus-based applications that offer more possibilities of storing and using the blockchain technology (Buterin, 2014, p. 13).

Hash or hashing is the process by which a grouping of digital data is converted into a single number, called a hash (Norton Rose Fulbright, 2016).

Internet of Things (IoT) – is the resulting global network interconnecting smart objects by means of extended Internet technologies and a set of supporting technologies necessary to realize such a vision (Miorandi, Sicari, De Pellegrini & Chlamtac, 2012).

Mining – “the act of contributing computing power to the network” (Benton & Radziwill, 2017, p. 39)

Multisig – multisignature. “aim to create a primitive dispute resolution mechanism allowing anonymous parties to settle a conflict without referring to courts or external arbitrators” (Cuccuru, 2017, p. 183).

Permissionless blockchains – “anyone can participate in the verification process” (Peters & Panayi, 2015).
Permissioned blockchains – “verification nodes are preselected by a central authority or consortium” (Peters & Panayi, 2015).

Private blockchains – “permission is restricted to users within an organization or group” (Peters & Panayi, 2015).

Public blockchains – “anyone can read and submit transactions to the blockchain” (Peters & Panayi, 2015).

Smart contract – “an agreement in digital form that is self-executing and self-enforcing” (Werbach & Cornell, 2017, p.320), “A computer program which verifies and executes its terms upon the occurrence of predetermined events” (Giancaspro, 2017). “Uses the blockchain publishing platform to run computations which determine how financial assets are managed” (Davis, 2014).

Third parties – companies or organizations that are related to blockchain, smart contracts, the insurance industry, IoT or AI.
2. Literature Review

*The purpose of this chapter is to provide the theoretical background about blockchain, smart contracts, the insurance industry and functionality of third parties.*

To understand what areas are included in the topic of this study, it is necessary to recognize the background and technical functionality as well as the processes behind the areas of interest. In this section, the areas will be described from the aspects of history, and utility using previous research on each area.

2.1. Blockchain

Blockchain as a concept was first described in 1991 when two researchers suggested cryptographic procedures to digitally timestamp a digital document, so it would not be possible to back- or forward date the document (Haber & Stornetta, 1991). Though it was not until 2008 when the whitepaper about Bitcoin by Satoshi Nakamoto, the word “Blockchain” started being used worldwide (Benton & Radziwill, 2017; Nakamoto, 2008). Nakamoto (2008) created the cryptocurrency called Bitcoin which was the first cryptocurrency used by people and is also the most well-known, but as in many cases the first version is not always the best one. Bitcoin and its implemented blockchain version has its limitations. The amount of information that can be stored in a Bitcoin block is relatively small compared to the blockchain platforms that can contain executable code like for example Ethereum which is considered a Blockchain 2.0 platform.

Blockchain is built on the Distributed Ledger Technology (DLT) which in reality is just a database containing digital or physical assets that can be shared in a network throughout many institutions and geographical locations. The idea is that all members of the network must have their own identical copy of the ledger (Walport, 2016) hence the word *Distributed Ledger* in the name of the concept. The purpose of the blockchain is to use
To secure the assets and make sure that the digital information stored in the blockchain is accurate and untampered with, cryptography is used.

“The global economic system depends on that individuals and organizations trust other entities to create, store and distribute essential records” (Beck, Avital, Rossi & Thatcher, 2017, p. 381)

A blockchain can be considered as a ledger, a chronological database of transactions where the transactions are stored in blocks (Peters & Panayi, 2015). A blockchain is an encrypted database that is immutable and thus cannot be corrupted. This is the essence of the blockchain, to offer storage to transactions in a ledger that cannot be corrupted means it can be trusted and this trust is built without the influence of a central authority (Benton & Radziwil, 2017). The Blockchain is decentralized (Figure 1) and it is called a blockchain because it can be viewed as a chain of blocks interlinked with mathematically calculated data using specific algorithms, also known as cryptography.

Figure 1: Decentralized blockchain. Courtesy of followmyvote.com
Each block in the chain contains (Figure 2):

- the address to the previous block, that is the root hash of previous block
- its own address or root hash based on the hash calculation of all transactions within that block
- a timestamp, when the block was added to the blockchain
- a nonce, a random number used for verifying the root hash

(Nofer, Gomber, Hinz & Schiereck, 2017)

![Diagram of a block in a blockchain](image)

**Figure 2: Simplified model of a block in a blockchain. Courtesy of themarketmogul.com**

The first block in the blockchain, the Genesis block, is hard-coded in the source code on the blockchain nodes. Each block in the chain can be validated by following the trail of hash numbers located in each block, that is following the addresses of each block to the previous block (Buterin, 2014). Successfully following the chain from block to block and verifying that each block contains the hash of the previous block means the chain and its contents are validated and unaltered. When new data is entered into the blockchain, it must first be verified by the participants in the blockchain system and this can only happen when there is consensus between them all (Mearian, 2017).

Each time a new block is to be added to the blockchain, the hash of the new block needs to be calculated. A new block is added every X minutes (for example, 10 minutes for
Bitcoin) and this is done by “miners” who compete to solve a difficult mathematical problem based on the cryptographic hash algorithm for that specific blockchain. The first one that solves the puzzle has mined the block and is rewarded a certain amount of the cryptocurrency which the blockchain is connected to. This calculation and validation of the blocks in the blockchain is called proof-of-work (Benton & Radziwill, 2017).

Like the state of the Internet can be divided into many versions so can the state of the blockchain technology. Blockchain 1.0 was introduced to offer digital currencies in the shape of cryptocurrencies where the "money" could be mined using computers to search for strings of codes that fit in a mathematical algorithm. Blockchain 1.0 focuses on the deployment of cryptocurrencies in the applications related to cash such as currency transfer, remittance and digital payment systems (Swan, 2015).

Furthermore, Blockchain 2.0 consists of contracts, economic, markets and financial applications that use blockchain beyond cash transactions. Example include smart contracts, smart property, stocks, bonds, loans, mortgages, land and property titles (Swan, 2015; Scott, Loonam & Kumar, 2017).

Blockchain 3.0 consists of different applications that do not involve money, currency, financial markets, commerce and other economic activities. Examples of such applications include; health, science, digital identity, governance, education and various aspects of culture. The most promising application of blockchain technology is smart cities which consists of different infrastructure such as smart governance, smart mobility smart use of resources as well as smart economy. It is possible to implement the transaction of smart property using internet of things and peer to peer (P2P) trade based on blockchain and smart contracts (Efanov & Roschin, 2018). Table 1 shows a summary of the different generations of Blockchain.
Generations of Blockchain | Areas of applications
---|---
Blockchain 1.0 | Currency transfer, remittance and digital payment systems
Blockchain 2.0 | Smart contracts, smart property, stocks, bonds, loans, mortgages, land and property titles
Blockchain 3.0 | Health, science, digital identity, governance, education

| Table 1: Generations of blockchain |

### 2.2. Public and Private blockchains

Blockchains can be either public or private. In public blockchains any participant has the right to create and send transactions and write blocks of transactions to the ledger without the permission of higher authority. The consensus process of grouping blocks of transactions is controlled by authorized nodes. On the other hand, private blockchains limit participants to write to the blockchain. A private blockchain, also known as permissioned blockchain, allows known participants within a group or organization to write data to the blockchain and denies of read and write to non-members (Xu, Pautasso, Zhu, Gramoli, Ponomarev, Tran & Chen, 2016). Private blockchains can for example be used by companies that are interested in storing information in an immutable ledger where only certain authorized people can add information to the blockchain.

### 2.3. Benefits of blockchain

According to an earlier study (PWC, 2017), it is argued that blockchain technology will offer a range of benefits to the insurance industry including the following;

- Blockchain technology will facilitate automation of processes thereby eliminating the need for input in some areas of operation. For example, the Allianz group uses a system based on smart contracts (natural catastrophe swap) to improve
claim management thus reducing human input. When an event happens, that meets the terms and conditions of the contract, the smart contract automatically executes payments to all affected parties with catastrophe insurance.

- Furthermore, blockchain technology will lower the risk of fraud and theft of insured property through creating a global tamper-proof registry. For example, Everledger uses blockchain to create a global registry for precious stones. This digital ledger tracks and protects valuable assets throughout their lifetime journey. It records an asset’s defining characteristics, history, and ownership to create a permanent record on the blockchain. Various stakeholders use this digital thumbprint, across a supply chain to verify the original and the authenticity of the asset.

- With continuous compilation of behavioral risk factors by insurers through connected and exchanged on the blockchain, prices will be adjusted based on real time information. The assessment of customer behavior and risk profile will result in better pricing and customized insurance products proper risk management. The study notes that underwriting, pricing and claim management processes will become faster and more efficient by deploying rules through the smart contract leading to better solutions offered.

- Blockchain will facilitate collaboration between insurers and banks thereby integrating different systems to a single platform and using data stored in the various systems of the banks for instance those relating loan applications and life insurance enrolment. For example, the Know Your Customer (KYC) platform developed by Mutuel Arkea group and IBM aimed at improving the sharing of customer data between banks and Insurance industry. In this case therefore, blockchain lowers costs by reducing the need for employees working on KYC tasks thus shortening processing time and improving customer satisfaction.

- Blockchain will enable new markets whereby insurers will be in position to develop and customize products and services thus providing a competitive insurance offer. This study also reveals that an insurance industry will offer payouts in real time in the event of the claim covered. Berkshire Hathaway Travel protection developed this innovative solution for insurance industry. This solution involves an insurer connecting to an airline system to retrieve information about
flight delays or cancellations and identifies customers affected through a customer database. The smart contract triggers the claim thus prompting payment to the affected customers.

In addition to the above, blockchain will improve efficiency, decrease the costs of transaction processing, boost experience, improve data quality and increase trust between parties. Agents and third parties do manual processing of data leading to duplication across the value chain. Human error and differences due to data timeliness are persistent challenges. Smart contracts will eliminate these challenges by verifying the coverage and payments for agents and third parties. Smart contracts will settle claims using the coverage information recorded on it thus avoiding disputes and the need for extra reviews by claims insurance agents. This will lead to automation of claims payments (KPMG International, 2017).

Related to the above is the fact that smart contracts will streamline various processes stored on different systems and databases by automating authentication and computational processes (Hans, Zuber, Rizk & Steinmetz, 2017).

Furthermore, smart contracts have the potential to provide customers and insurers with the ability to manage claims in a transparent and responsive manner means. Contracts and claims stored on a blockchain could be validated through the network thus ensuring that only valid claims are paid. For instance, if multiple claims involving one accident are submitted through blockchain, the network would know that the claim had already been made. Therefore, smart contracts would enforce the claims by triggering payments when certain conditions are validated (Deloitte, 2016).

Blockchain technology will improve customer engagement and satisfaction whereby if the data is digital and verified, customers will not need to submit documents more than once. The transparency of transactions will improve fraud monitoring and detection, that is, the insurers will access claims on a shared network, verify them and be in position to identify any fraudulent claims. In addition, insurers can automate the claims process by
integrating with third party vendors and managing claim through a consortium network of insurers (Crawford, 2017).

2.4. Challenges and limitations of blockchain

It has been previously stated that a blockchain is immutable and cannot be changed. This is not entirely true as even the blockchain technology has its weak spots. Although the Blockchain offers very secure and almost incorruptible storage of data there are limitations to its use. Just because there is a transaction on the Blockchain does not mean that it is an actual or correct representation of an interaction between two parties. People can still be fooled or misled into signing deals (Benton & Radziwill, 2017).

There are security issues with the blockchain such as the 51% attack. In this attack, one mining entity can take control of the blockchain and double spend the previously transacted coins to his or her account. This occurs when the mining of coins is centralized such as there is competition to record or write new blocks in the blockchain. In other-words only few large mining pools control the majority in the transaction recording (Swan, 2015). Bradbury (2013) notes that 51% attack results to a fork (duplication of processes) where two conflicting blocks compete to be written to the blockchain. The author claims that if the majority of the mining power on the network supports the attacker's block, the same block can be sent to the blockchain resulting in fraudulent transactions.

Another thing is that it is still difficult to enforce one party to comply to a contract. For example, even though you can prove that a person owes you money it could be difficult to get the person to actually make the payment (Benton & Radziwill, 2017), unless a smart contract is used to automatically move cryptocurrencies from one wallet to another after the fulfilment of a contract.

A public blockchain is distributed which means that there are copies of the blockchain in many different places. As more blocks are added on the blockchain, the space available becomes less since few nodes will contain the entire blockchain. This is the scalability
problem of Blockchain (Benton and Radziwill, 2017) and must be solved in the future if Blockchain is going to be used on a global scale. For example, let’s say that the Blockchain has reached the size of 100 TB. Very few individuals have this storage capacity which means there must be sponsored organizations or companies that spend money on keeping this infrastructure of hardware and networking up and running.

The proof-of-work process is very costly from an energy point of view. As stated before, mining a block is a competition and only the first miner is rewarded for its contribution. The rest of the miners have used electricity in vain and this wasted energy resources is a huge problem already. The electricity consumption for mining on the Bitcoin blockchain was estimated to equal that of the country of Ireland (O’Dwyer & Malone, 2014; Walport, 2016). As the use of the blockchain technology would increase so would the energy consumption and this is of course not sustainable.

Standardization of blockchain systems is critical to realizing the benefits of blockchain technology. The lack of standards and proven successfully implementation of blockchain technology justifies that the technology is still in its early stages. Therefore, there is a risk of implementing inefficient solutions if pre-implementation efforts are not defined as well as well established industry standards (McKinsey&Company, 2016). According to an earlier study (Mainelli & Manson, 2016), it is argued that using unpermissioned systems where any person can access the system which results to not knowing the contracting parties thus creating a challenge of enforcing regulations. The current regulators impose rules on entities but not systems or networks.

Blockchain is affected by high latency whereby it takes time of a verified block for transactions to be added to the ledger for instance Ethereum takes 17 seconds to verify a block of transactions which is then added to the ledger (Ream, Chu & Schatsky, 2016). There are however solutions to this. The Lightning Network which is a solution for increasing the transaction speed and scalability for the Bitcoin blockchain, is one example (Lightning Network, 2018).
2.5. Smart contracts

A smart contract is a set of promises specified in digital form, including protocols within which parties perform on these promises (Szabo, 1996). According to this same author, a smart contract is both an instance of computer code and a running software program that interprets the code, accepts input conditions and decides on the outcomes.

Murphy and Cooper (2016) state that a smart contract has four key characteristics. These include the following:

- Digital form – it is code, data and running programs
- Embedded – contractual clauses or functional outcomes are embedded as computer code in software
- Performance mediated by technological means – the release of payment and other actions are enabled by the technology.
- Irrevocable – once initiated, the outcomes for which a smart contract is encoded to perform cannot be stopped unless if an outcome depends on unmet condition.

Smart contracts are programs stored in the blockchain that can be run with a guarantee that it will always respond when invoked and it cannot be censored or altered according to Buterin (2014).

“Smart contracts are a step beyond typical electronic contracts in that the actual agreement is embodied in computer code, rather than English or another traditional language” (O’Sheilds, 2017, p.181)

When a smart contract is created, the parties must first agree on the contents (Sillaber & Waltl, 2017). All parties in the contract must have wallets in the blockchain the smart contract is added to. The parties of a smart contract are represented by the private keys of the parties (Sillaber & Waltl, 2017). When the contents are agreed upon, the smart contract is submitted to the blockchain as a transaction in a block through the usual
process of mining. After the block has been added, the smart contract is ready to be run and when a smart contract is invoked, it runs the input data and checks if the conditions for triggering one or more events, are met. If the conditions are met, then the new transactions are added to the blockchain (Sillaber & Waltl, 2017).

The behavior of a smart contract is decided by the programmer of the smart contract. It is the responsibility of the programmer to make sure that the code in the smart contract is an actual representation of the intended transaction of the parties (Benton & Radziwill, 2017).

It is stated that smart contracts might replace the need for courts to replace smart contracts (O’Shields, 2017).

“As autonomous business agents advance through smart contract formation and enforcement protocols, blockchain technology will reduce the risk and accelerate the implementations of e-commerce driven by artificial intelligence” (Robey, 2017, p.20)

2.6. The difficulties of smart contracts

From the legal perspective, the use of smart contracts raises various issues. Parties involved in the smart contracts may be anonymous. For example, one party may sign an agreement with a minor. This creates a risk of the enforceability of the agreement. Although there are procedures to determine the age before the entry of a transaction on the blockchain, it may be difficult for the police to investigate such a scenario. It raises a question whether such a contract would be binding (Giancaspro, 2017).

Managing financial and asset exchanges through a smart contract may raise an issue especially if the programmable logic and code (representing the terms and conditions) is not understood by either of the parties in terms of how it behaves. Another issue is when parties share an external document containing all legal terms and conditions that will bind the parties and reflect the way the smart contract will behave. The issue in contention is
whether the external document will reflect the way the code will behave. In case of any mistakes in the code, the parties should agree mutually. The parties should seek court order requesting modification of the code of the smart contract reflecting their actual intention (Ryan, 2017).

The execution of a smart contract does not fit in the traditional basis of territorial jurisdiction thus making it difficult to determine which laws will apply to govern contractual issues related to a specific smart contract. More still, there is a challenge to determine which court has the jurisdiction to hear legal claims resulting in the use of smart contracts (Sherborne, 2017). The author notes that it is difficult to resolve and arbitrate disputes arising from the performance of the smart contracts, for instance, if one of the party contests whether a smart contract is legally binding. The fact that there is no central enforcement agency, it is difficult to predict with certainty how such an issue can be resolved.

2.7. Smart contract blockchain platforms

There are many blockchain platforms for creating smart contracts. They are all created for different purposes and by different organizations. The blockchains that will be discussed here are Ethereum, Hyperledger Fabric and the DLT technology Corda. The reason these three were selected is because the first is public, the second is a private blockchain and the third one is not actually a blockchain but a DLT technology created by R3, a consortium of financial institutions.

2.7.1. Ethereum

The intention of the Ethereum platform is to merge previous work on the blockchain technology together with new functionality to improve scalability, standardization, ease of development and interoperability with other platforms. It is a decentralized platform with the functionalities of smart contracts. Its cryptocurrency is “Ether” used for payment of transactions and the programming language used for creating smart contracts in Ethereum is called Solidity (Buterin, 2014). Although being a widely used platform,
Ethereum might not be the best choice for smart contracts (Egelund-Müller, Elsman, Henglein & Ross, 2017). To start with, the computational cost, or *Gas* as it is called, is high and there are performance issues. Finally, Ethereum is a public ledger which means the transactions can be visible to anyone (Egelund-Müller et al., 2017).

### 2.7.2. Hyperledger Fabric

Hyperledger Fabric is a permissioned blockchain based on the Hyperledger Project and allows the running of smart contracts (Cachin, 2016). Hyperledger Fabric allow the distributed applications to be written in general-purpose programming languages and are not dependent on the cryptocurrency of the platform. However, the programming language used in the smart contracts is Go (IBM, 2018).

### 2.7.3. Corda

Corda is not a blockchain but a distributed ledger platform designed for the financial sector. It is a platform that can be used to develop applications for the financial institutions. It's also a permissioned private network intended to record, manage and synchronize financial agreements or contracts between regulated financial institutions. Corda can remove costly payments in business transactions by avoiding business intermediaries and focusing on the financial domain. Corda allows for the creation of immutable records for financial events. Corda smart contracts can be written in Java or another Java virtual machine language. Corda has a simple architecture that boosts its performance and security over other enterprise level frameworks (Blockchain Expert, 2017).

### 2.8. Oracles

Smart contracts contain code that can be triggered by external input but because of the blockchain consensus protocol, smart contracts cannot communicate directly with external systems (Ellis, Juels & Nazarov, 2018). Instead this communication is done by
so called oracles. An oracle is a software artifact that have API’s to smart contracts in the blockchain and also API’s to external trustworthy information (Figure 3). Some oracles are distributed and decentralized that will work as intermediaries between the blockchain and trustworthy sources of data. These trustworthy data sources must have API’s so that oracles can fetch information from them. An example of a trustworthy source is the weather agency in Sweden, (SMHI, 2018) which offers API’s.

Smart contracts can be triggered by requesting information from the oracles using the oracle API. The oracle in turn requests information from the sources using the sources API. The data received in the smart contract is tested and if the data does not fulfill the requirements of the code, nothing happens. But if the data fulfills some part of the smart contract code, then this part of the contract is triggered and the pre-decided contract events will be triggered (Ellis, Juels & Nazarov, 2018).

![Figure 3: Oracles communicate with different sources. (www.smartcontract.com)](image)

Even though the communication between the smart contracts and the oracle is encrypted there is really no way of guaranteeing that the information sent to the oracle and passed on to the smart contract is correct. Since the sources are considered trusted there is no need to double check, but even trusted sources can be compromised. Detectors can be tampered with and measurement equipment can malfunction. If the smart contract gets the wrong data, it may trigger an event when it is not supposed to and this may lead to insurance fraud being committed. This can be solved with so called majority voting. This involves requesting the same information from many different sources and if the majority
of the sources sends the same data, it can be considered to be trustworthy (Ellis, Juels & Nazarov, 2018).

2.9. DAOs /DACs

Decentralized Autonomous Organizations (DAOs), also known as Decentralized Autonomous Corporations (DACs) are defined as virtual entities on the blockchain that consist of members that have the right to spend the funds contained within the entities or modify the code that make up the entities and their functionalities (Buterin, 2014).

The blockchains behavior may be modified if only a certain process programmed in the contract is followed. For example, a smart contract that calls another contract by address to perform its main function. This contract consists of members’ list, addresses (public keys) that decide on its behavior (Christidis & Devetsikiotis, 2016).

“These new technologies make it possible for a group of independent parties to work with universal data sources, automatically reconciling between all participants – customer, broker insurer, co-insurer, reinsurer, all having a distributed and single view of the entire exposure data chain” (Nath, 2016)

2.10. Use cases of blockchain in the insurance industry

According to an earlier study by KPMG International (2017), it is argued that blockchain will offer various business opportunities to the insurance industry in terms of products and services. Some of the potential use cases of blockchain technology according to this study include:

- Travel and life insurance - companies will develop pay-as-you-go insurance model that will provide instant payouts in the event of delays or cancellation.
• Claims management - companies will automate the verification of coverage and streamline claim settlement thus improving operational efficiency and reducing cost.
• Personal accident insurance - companies will create a transparent and an all-in-one claims journey that will improve customer satisfaction.
• Record keeping - companies will create, organize and maintain records in a single, reliable and accessible database.
• Reinsurance claims - companies will be able to automate straightforward claims triggered by smart reinsurance contracts and models.
• Digital identities - companies will use blockchain data and digital ledgers to digitalize and validate customer information thus improve compliance.
• Peer-to-peer insurance - companies will build peer-to-peer network to establish smart contracts without the need for an intermediary.
• Surety insurance - companies will create a wealth source of information on surety bonds accessible in real-time to all members.

2.11. Insurance brokers and Agents

Insurance brokers provide information to potential insurers that help them in risk management. In cases where the risks are too complex to be insured by one company, the broker transfers the risks to other insurers who are willing to take up the insurance coverage. In this case, the broker spearheads the negotiation process by determining the design of insurance coverage, pricing on behalf of the policy holder. Insurance agents provide services to clients such as claim management, insurance coverage design and offer advice based on the clients’ insurance needs (Cummins & Doherty, 2006). Furthermore, insurance agents provide post contract customer services such as changes in payment methods, beneficiaries and other terms of service. They also provide basic legal, health, tax and financial information thus increasing customer satisfaction. (Lee, Cheng & Cheng, 2007)
3. Theoretical framework

This chapter explains the core of Contract Theory and its relation to smart contracts. The purpose is to allow the reader to understand the chosen perspective of this study.

Technology is taking up more and more space in our everyday lives as technological innovations transform the societies we live in. This can be observed by comparing how we use technology today and how it was used in the previous decades. As society becomes more dependent on technology, we must also adjust the rules and regulations that come with the technical progress.

“Advances in computer science and information systems research have now created technologies that are supposed to have the potential of reshaping wide areas of the legal system as it is established nowadays. Especially contractual law seems to be highly suitable for digitization” (Sillaber & Waltl, 2017)

Although smart contracts in many cases only will work as autonomous agents triggering an event or a series of events, in some cases smart contracts also will work as legal agreements, which is of much interest. To find out exactly how and if smart contracts would be considered to be legally binding contracts, it was important to learn how classic contracts work and what theory these contracts are applicable to. For these reasons, we believe that contract theory will have the biggest impact on the rules and regulations surrounding the notion of smart contracts and thus was chosen as the theoretical framework for this thesis.
3.1. Contract theory

The traditional definition of a contract is a set of promises between two parties which the law will enforce. Contract theory states that the contract law “[…] should facilitate the efforts of contracting parties to maximize the joint gains […] from transactions” (Schwartz & Scott, 2003, p. 544) and nothing else. What is not listed in the contract should be handled by the law in the country. This means that it is first and foremost up to the parties of the contract to uphold their set promises.

A contract is an agreement between two parties. Contracts are promises that can be enforced by the law when the promises are not kept (Cornell Law School, 2017). The involved parties can for example be state registered organizations or individuals and for the agreement to be legally binding it must fulfill four requirements (Figure 4). According to Schwartz and Scott (2003) there must be:

1. Mutual assent – one party must have an offer and the other party must accept
2. Adequate consideration – money, an act, property, a promise to do or not to do an act
3. Capacity – A legal right, power or knowledge to perform an act. An ability to understand the act and the consequences of the act.
4. Legality – The state of conforming with the law. For example, a court cannot enforce the fulfilling of an agreement where one agrees to sell illegal drugs to someone (Levy, 2017, p. 6).

In addition, there are few more so-called defenses to enforcement of contract (O’Shields, 2017) as seen in Table 2.

<table>
<thead>
<tr>
<th>Mistake</th>
<th>Undue influence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misrepresentation</td>
<td>Unenforceability</td>
</tr>
<tr>
<td>Duress</td>
<td></td>
</tr>
</tbody>
</table>

*Table 2: More defenses to contract enforcement*
To understand the cases and the different laws that apply, contract theory uses four categories to understand the theory. There must be a seller and a buyer for a transaction to take place (Figure 5). These parties are represented by firms and individuals and the transactions between them can be divided into four categories (Schwartz & Scott, 2003):

1. A firm sells to a firm
2. A person sells to a person
3. A firm sells to a person
4. A person sells to a firm.

![Figure 4: The four elements of a valid legal contract](image)

<table>
<thead>
<tr>
<th>Mutual assent (offer-acceptance)</th>
<th>Adequate consideration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity</td>
<td>Legality</td>
</tr>
</tbody>
</table>
The laws that apply to a certain category depends on whether the transaction is in regard to a service, product or asset. For example, category 2 contracts that are about services or products switching owners is handled by Köplagen in Sweden (Sveriges Riksdag, 1990) whereas a category 3 contract is handled by Konsumentköplagen when a product is sold to an individual (Sveriges Riksdag, 1990) and Konsumenttjänstlagen when a service is sold to an individual (Sveriges Riksdag, 1985). If a company sells something over the internet, then the consumer is protected by another law called Distansavtalslagen which among other things gives the consumer a time period of 14 days to return a product if unused. Service that have already been consumed within this time can of course not be returned (Sveriges Riksdag, 2005). In general, contract law is common through many states but there may be different court interpretations on certain parts of the law from state to state (Schwartz & Scott, 2003).

Breaches
Contract law also involves breach of law, meaning that one party has not performed the agreed upon act. Breach of law can result in financial losses or missed opportunities for the other party and according to contract law, breach can lead to a lawsuit in general court if there are no clauses in the contract that handles breaches (LII, 2017).

Self-enforcing contracts
Most contracts will be performed by the parties even if there are no legal consequences for a breach. Contracts like these are “self-enforcing” in two ways:
- If the parties of the contract can gain more by performing their part of the deal than if they break the deal.
- If the cost of the parties’ lowered reputations is higher than the gains of the breach.

When a contract is not “self-enforcing” it is up to each party to have breach clauses in the contract. In case of a breach of contract, these breach clauses specify what will happen, that is what the breaking party must do instead. Many times, it means the breaking party must pay a fee and it is not unusual that this happens. If the cost of contract breach for some reason would be cheaper than to perform the promises of the contract, then one party can break it and pay the breach fee instead. However, in case there are no breach clauses or the breaching party does not abide to the breach clause, a lawsuit will be handled in court (Schwartz & Scott, 2003).

3.2. Smart contracts and contract law

A frequently asked question when it comes to smart contracts is whether they are actual contracts. The answer is that smart contracts can be both autonomous agents and legally binding contracts, although not at the same time. Only a few of the smart contracts will be legally binding (Norton Rose Fulbright, 2016) as depicted in Figure 6. Only the ones that fulfill the requirements of a legal contract according to contract law, will be used as actual contracts.

![Figure 5: Smart contracts are only legal contracts in some cases. Courtesy of Norton Rose Fulbright (2016).](image-url)
A contract is a legally enforceable promise or promises. For a contract to be legally enforceable, it must meet various conditions imposed by the law like mutual assent, consideration, intention to create legal relations (capacity), and certainty of terms-legality (Norton Rose Fulbright, 2016). In order to enforce the smart contract, the contract must meet all the traditional requirements of a valid contract. Mutual assent must be evident by making a promise or yield performance (O'Shields, 2017). The parties to the contract base mutual assent on the concepts of offer and acceptance. In order to enforce a smart contract, there must be a clear record of mutual assent to the terms and the terms must be disclosed to the parties in the contract.

Both traditional and smart contracts have bargain for consideration. For example, in traditional contracts the courts believe that mutuality of obligation can differentiate a contract from a gift where parties do not have the same legal right of enforcement. On the other hand, smart contracts can formalise contracts since the terms are clearly laid out and each party’s obligations and benefits are specified. In a smart contract, the bargain can be presented unilaterally, like for the case of the vending machine or can be bargained for through terms and conditions of the loan agreement (Raskin, 2016).

Raskin (2016) asserts that the common law doctrine of substantial performance permits a contract to be recognised even if the performance does not fully conform to the terms laid out. On the other hand, a smart contract cannot recognise such contract because the outcome is different from the specified terms and conditions in terms of performance. This can be dealt with if parties include a certain degree of discretion in the terms and conditions of the contract before it is formed. In circumstances where the terms are different from what the law recognises, then the parties must seek court’s jurisdiction to solve this issue. There are two instances where the law pardons a party from performance or modification of the contract, that is impossibility and impracticability. For example, if a smart contract becomes illegal after it is formed then the parties can be excused of performance.

Furthermore, Raskin (2017) raises an issue of breach of contract whereby the outcomes of the smart contracts are totally different from the contract law and do not comply with what the law requires. Raskin (2017) also raises an issue of breach of contract whereby
the outcomes of the smart contracts are totally different from the contract law and do not comply with what the law requires. In this case, courts will enforce smart contract terms since they will assess the terms of both parties clearly stated in the contract. Smart contracts will be written in such a way that accommodates future changes in the law.

Talking about smart contracts and Contract Law is easy, making it happen is much more complicated. According to Tjong Tjin Tai (2017) it is difficult to employ smart contracts that are able to correct mistakes. Smart contracts are pieces of code in a blockchain and they are supposed to be immutable, but this does not rhyme well with contract law where corrections are an important part. This limitation is an important aspect one must consider when creating smart contracts. Furthermore, Tjong Tjin Tai (2017) states that in order for smart contracts to be seen as “code as law”, that is law in the form of computer code, several issues must be taken into account:

- Legal expertise will not be needed when creating smart contracts
- Automated payments would be done using digital currencies not handled by traditional banks or third parties.
- Automatic execution of contracts could be done without the need of external legal enforcement and there should be no interference from any party.
4. Research methods

This chapter will explain the authors’ selected research approach and why the particular research methods were chosen.

This interview study intended to explore the opportunities and challenges the insurance industry faces with the emergence of blockchain technology and particularly the use of smart contracts.

4.1. Research approach

The study was based on a qualitative research consisting of an in-depth interview and a structured questionnaire. Both inductive and deductive research approaches were used on the data collected. It started with gathering of data from interviews with selected interviewees. Analytic induction was used to analyze the qualitative data to identify the condensed meaning unit, codes, categories and themes in the interview transcripts that were related to the purpose of the study. The data was saved in an excel sheet and the analysis commenced with a close reading of the text.

The themes from the interviews were explored further to formulate a questionnaire that consisted of in-depth questions related to the themes of the theoretical framework (contract theory). To get a deeper understanding of the research topic, more questions were formulated based on other themes for example, opportunities and challenges of smart contracts. Regarding the questionnaire, the responses were analyzed using deductive content analysis. The interview-guide to the questionnaire can be found in Appendix B.
4.2. Research setting

Three interviews were held with representatives from the blockchain community. This was followed by another three interviews consisting of different interviewees from a Swedish nationwide insurance company.

The first interviewee from the blockchain community was a conference speaker who had general knowledge about the blockchain technology and its use cases. The second interviewee was a lawyer specialized in IT and blockchain issues. The third interviewee was a communications manager who works at an oracle company.

The insurance company cover all Swedish counties and has offices in all major cities and some selected towns. They offer all kinds of insurances, from personal to associations and companies. The three insurance representatives interviewed consisted of: the head of sales, an insurance conditions manager and the head of vehicle damages.

4.3. Methods of data collection

Our methods of data collection consisted of interview data and information from peer-reviewed research articles, white papers and consulting reports.

4.3.1. Secondary data collection

We collected secondary data by searching for books, peer reviewed articles, journals, consultancy reports and white papers. We asked ourselves what type of search phrases we could use to find and gather the information needed to answer the research questions. We searched Jönköping University online library (Primo), online databases such as Scopus, Proquest, Google scholar, Emerald, ACM digital library and Google search engine. We used a combination of search phrases as shown in Table 3 to find relevant articles for our literature review.
When the search results appeared, we scanned the abstracts of the articles in the results and selected in total 100 articles and books to read through. After reading through the articles, journals, white papers, consultancy reports and parts of the books, we selected and used a total of 60 articles that were relevant to our research.

### 4.3.2. Sampling techniques

Both purposive sampling and snowball sampling techniques were used because individuals who had knowledge and experience from blockchain technology, contract law or the insurance industry or preferably a combination of the areas mentioned, were needed
to be found. This sampling technique helped us to first select interviewees with expert knowledge and experience in blockchain technology and contract law.

We then used snowball sampling to find even more potential interview candidates. By connecting with people who had specific knowledge in our area of research, it was easier to connect with other people who were recommended to us by our connections. Some of these new connections were interested in sharing their experience and expertise through our interviews. To find people with experience in the blockchain and insurance industry, we used social media, primarily LinkedIn, but also Facebook and Twitter to connect but we also spent considerable time sending emails and making phone calls.

For example, through LinkedIn we searched for people who worked with Blockchain, smart contracts or worked in the insurance industry by using the search phrases: “blockchain”, “smart contracts” and “insurance” as well as combinations of these keywords. This resulted in a good base of people who were either in the industry or knew someone who could better answer our questions. We made connections with many of these people and by sending private messages to selected individuals and asking for permission to interview them, we encountered a few people that we later interviewed.

Furthermore, through Facebook we accessed open groups as well as applied for membership in closed groups and advertised for people to interview that had knowledge in the Blockchain technology. We got our first interview with a conference speaker that gave lectures on blockchain technology. This person responded to our post in the swedish Facebook group named “Kryptovalutor & Blockchain Sverige - Bitcoin, Ethereum, Litecoin m.fl.”.

By searching for the names of the CIO’s at the big insurance companies and some banks in Sweden we found the people we wanted to contact for an interview. We then sent connection requests on LinkedIn where we presented ourselves and explained the reason why we contacted them. To those who accepted our connection requests, we sent private messages to and asked them for interviews or if they could recommend other people that would be interested in being interviewed. We also sent emails directly to some of these
C-level executives (Chief Executive Officer, Chief Operations Officer and Chief Financial Officer).

In addition, we made phone calls to insurance companies in Sweden. We called the headquarters and got the email addresses to the CIO's upon where we sent emails describing the purpose of us reaching out to them but sending emails to the CIO's resulted in mostly nothing. Only one CIO got back to us with an email address to their Head of Innovation.

We emailed two oracle companies, which resulted in an interview with the communications manager at one of the companies.

4.3.3. Interviews

We used in-depth interviews in order to explore general views about blockchain and smart contracts. However, some specific questions were asked depending the interviewee’s background. This provided a broader understanding of the research topic and helped us to meet the overall purpose of the research. (Refer to Appendix A).

The reason why interviews were chosen for this study was that there are not many research papers about the use of smart contracts in the insurance industry. In addition, few platforms allow for the use of smart contracts. Another reason is that blockchain technology is relatively young and only few platforms utilize smart contracts. Most industries have not yet embraced this technology and therefore few examples of case studies or research papers exist.

Since the topic on Blockchain is relatively new, there is limited information available on our topic. To acquire information on the topic from different perspectives we had to interview people with different backgrounds in the blockchain industry. Therefore, we had to formulate an interview guide with questions specific to each of the interviewees.
This resulted in interviews with representatives from different backgrounds related to blockchain technology and smart contracts. The blockchain technology and smart contracts were explored from different perspectives such as:

- The technological aspect
- Legal validity
- Insurance perspective and
- Third party perspective

According to Saunders, Lewis and Thornhill (2016), it is argued that interviews provide valid and reliable data relevant to your research question and objectives. Taylor, Bogdan and DeVault (2015) emphasize key points in adopting a strategy of qualitative interviewing such as; asking open ended questions, descriptive questions about the general topic and experience of the interviewee. They also note that, asking specific questions about the interviewee’s experience and perspective enables the researcher to probe further by asking specific follow-up questions. This was evident during our interviews where we explored the topic further by asking follow-up or additional questions. This was aimed at creating clarity on certain themes or questions that seemed confusing. We recorded and transcribed the interviews using Callnote which is a software that records audio and video conversations for Skype, Facebook and Google+. 
<table>
<thead>
<tr>
<th>Position</th>
<th>Interview duration</th>
<th>Date</th>
<th>Interview type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Co-founder, speaker, Blockchain virtual, community</td>
<td>90 minutes</td>
<td>Feb. 16th 2018</td>
<td>Skype</td>
</tr>
<tr>
<td>IT Lawyer</td>
<td>77 minutes</td>
<td>March 9th 2018</td>
<td>Skype</td>
</tr>
<tr>
<td>Communications Manager at an oracle company.</td>
<td>59 minutes</td>
<td>March 17th 2018</td>
<td>Skype</td>
</tr>
<tr>
<td>Head of sales, insurance company</td>
<td>36 minutes</td>
<td>March 23rd 2018</td>
<td>In person</td>
</tr>
<tr>
<td>Insurance Conditions Manager, insurance company</td>
<td>30 minutes</td>
<td>March 23rd 2018</td>
<td>In person</td>
</tr>
<tr>
<td>Head of Auto damages, insurance company</td>
<td>40 minutes</td>
<td>March 23rd 2018</td>
<td>In person</td>
</tr>
</tbody>
</table>

Table 4: Summary of the interviews

4.3.4. Questionnaire

After an inductive analysis of the interview transcripts, we narrowed down the questions to acquire primary data from a questionnaire regarding the legal validity of smart contracts. These questions were open questions created to get a more in-depth understanding of the themes from the inductive analysis and the theoretical framework (Refer to Appendix B). The questionnaire was created using Google Forms and the link was sent to different respondents, including those we had interviewed, other selected contacts and forums on social media that were related to the blockchain technology and the insurance industry.

The purpose of the questionnaire was to gather data from respondents with expert knowledge about blockchain, smart contracts and the law. The questionnaire was based
on the theoretical framework addressing four major concepts such as; mutual assent, adequate consideration, capacity and legality in relation to use of smart contracts. The questionnaire comprised of other questions related to opportunities and challenges of smart contracts to the insurance industry and third-party companies. We sent the questionnaire to forty (40) experts with different backgrounds through LinkedIn, Facebook and other social media. The deductive analysis was based on ten (10) respondents.

4.4. Data Analysis

The data was analyzed using a conventional content analysis where the condensed meaning units, codes, categories and themes were derived from the interview transcripts. Graneheium and Lundman (2004) points out that the most suitable unit of analysis is whole interviews that are large enough to be considered as a whole and small enough to be kept in mind as a context of meaning units during the analysis process. Conventional approach to content analysis enabled us to gain direct information from interviewees without imposing preconceived themes or theoretical perspective (Hsieh & Shannon 2005). This method enabled us to explore as many themes as possible. We started by reading the transcripts and identifying words, sentences and paragraphs that we felt were important to our understanding of the topic. Furthermore, we used Microsoft Word to create condensed meaning units (text extract from the transcript) with codes. This procedure of writing codes was repeated several times for each interview transcript.

The condensed meaning units and codes were extracted to a new Word document using a macro and then copied to an excel document. The codes were then analysed and grouped into categories. The categories were analysed and grouped in to themes. Steps described by Elo and Kyngäs (2007); Erlingsson and Brysiewicz (2017) on how to conduct qualitative content analysis guided this process. This procedure was repeated for each interview. The analysis of the themes highlighted the common relationship among interviewees. Table 5 shows an example of how the themes were formulated.
<table>
<thead>
<tr>
<th>Meaning units</th>
<th>Codes</th>
<th>Category</th>
<th>Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;When they start the repair they might take away something from the front and it turns out that they have to replace more details that were impossible to see before&quot;.</td>
<td>Opportunity for Internet of things</td>
<td>Business opportunity</td>
<td>Insurance industry business model</td>
</tr>
<tr>
<td>&quot;Oracles will only get paid as they provide data to the contract&quot;.</td>
<td>Oracle service payment</td>
<td>Business opportunity</td>
<td>Third parties</td>
</tr>
<tr>
<td>&quot;The whole blockchain becomes huge and if you want to run a node you don't want to download 250 Gb.&quot;</td>
<td>Sustainability</td>
<td>Blockchain storage</td>
<td>Blockchain and IT systems</td>
</tr>
<tr>
<td>&quot;Well the difficulty with smart contracts is that they're actually very difficult to define from a legal perspective.&quot;</td>
<td>Challenge of smart contracts</td>
<td>Legal status of smart contracts</td>
<td>Regulations</td>
</tr>
</tbody>
</table>

Table 5: Formulation of themes from Interview transcripts.

By focusing on the themes from the interview that were related to theoretical frameworks, new in-depth questions emerged leading to the formulation of a structured questionnaire. The questions and responses were saved in a Google Spreadsheet file to make it easier to analyse. The questionnaire comprised of categories based on mutual assent, adequate consideration, capacity and legality. Other categories included: smart contract platforms, opportunities, challenges and limitations of blockchain.

Direct content analysis was used at this stage to validate the selected theoretical framework (contract theory). Hsieh and Shannon (2005) support this argument, which states that the main aim of a directed approach to content analysis is to validate or extend conceptually a theoretical framework or theory.
4.5. Research credibility

Credibility refers to the confidence in how well the collected data address the intended purpose of the research (Elo, Kääriäinen, Kanste, Pölkki, Utriainen & Kyngäs, 2014). Selection of the most appropriate method of data collection is essential for ensuring the credibility of content analysis (Graneheim & Lundman, 2004). We chose interviews as the most suitable method for data collection because they helped us to answer the research questions and meet the purpose of the study. This strategy ensured trustworthiness during the inductive content analysis. In addition, we evaluated how well the categories covered the data from the interviews and identified the similarities between the categories.

To ensure reliability, we minimized any factors or errors that would negatively affect the respondent’s performance during the interview session. For example, we decided to interview our respondents in the afternoon because they were happy, calm and relaxed thus producing better results as opposed to morning hours. Respondents’ bias was diminished by taking the interviews in a convenient environment or office. This ensured that interviewees expressed their honest opinions. To minimize researcher errors, we organized interviews at different dates thus ensuring proper interpretation of results. To minimize researcher bias, we interpreted the results from our respondents in an objective way.

From our interviews with individuals, directly or indirectly working with the blockchain technology, we received good answers to our general questions but a few respondents were not very familiar with contract theory and thus could not answer the more specific questions. Fortunately, they were very knowledgeable in their areas of expertise. The credibility of the interviewees that made the foundation for our inductive content analysis was high.

The number of respondents from the questionnaire was only ten, which is a low number to draw any conclusive conclusions from, but we still received some good answers. Some of the answers align well with the answers from our in-depth interview with the cybersecurity lawyer as well as with the literature.
4.6. Generalizability

To ensure external validity, we identified respondents using purposive and snowball sampling techniques. These techniques helped us gather data from respondents with good technical background about the opportunities and challenges of blockchain, smart contracts to the insurance industry and third-party companies. We were also able to gather data about the legal perspective of smart contracts. The focus of this study is not to generalize the findings to the entire population due to the limited number of respondents and interviewees. It represents the views of interviewees and respondents with technical working experience of the insurance industry, blockchain, smart contracts and law. Therefore, this study contributes to the existing theory by providing a diverse perspective of blockchain, smart contracts and law in a different research setting.

4.7. Research ethics

The communication to the respondents was made through emails and phone calls, clearly stating the purpose of the research and how the data gathered would be used. In this regard, we sought permission to record each respondent. In addition, we stated that the respondent’s name would not be published in this study. The duration of each interview was clearly stated and agreed upon with each respondent. We sought consent from each respondent before administering the questionnaire. The purpose of the questionnaire was clearly stated and how the data would be used in the study.

After each interview, we transcribed the recordings and sent them back to the interviewee to make sure that we had understood them correctly and that there were no misunderstandings. Most of the interviewees did not respond after mailing them the transcriptions but one interviewee mailed us back with a small correction.

After transcribing the interviews, we started analyzing them. The approach was to inductively analyze the text and select important parts of the text that we could interpret to codes. These codes were then the summarized to categories and finally into themes.
5. Results

The findings of the inductive content analysis performed on the interview transcripts and of the deductive content analysis performed on the questionnaire responses are presented.

This chapter is divided into two parts. The first part shows the results of the inductive content analysis based on the exploratory interviews. The second part shows the results of the deductive analysis based on the answers from the questionnaire.

5.1. Interviews

After an inductive content analysis of the interview transcripts, several categories were identified. This is because of the different backgrounds of the interviewees. For more details about the categories and themes for each interview, please refer to Appendix C.

Described below are the categories identified from the interview transcripts in support of the results.

5.1.1. Third parties

There is a potential for automating the process of life insurance using smart contracts. The insurance company prefers this policy because it is easy to manage. “Life insurance is a little easier because only if something happens to me in my life, that is, if I've deceased.” (Insurance Conditions Manager, at insurance company)

There is an opportunity for third party companies like oracles, for providing data to the smart contract as stated by the communications manager at the oracle company: “Oracles will only get paid as they provide data to the contract.” This also presents another opportunity for the node operators by providing “jobs” to the smart contracts. The
communications manager at the oracle company explains: “There must be an incentive like getting paid for providing the jobs and at the same time we need people to hear our family and ask for data that would be used to pay node operators”.

There are many ways to run a business. The organization, the goals and the business model may vary for example. With the rise of smart contracts there are several things that can help a company become more efficient. One of those things can be decision making. From the interview with the insurance company, it became clear that decision-making could be made easier by record keeping in the blockchain.

Smart contracts present an opportunity to companies using digital agreements. This will eliminate duplication of the digital agreement across different departments of the company thus reducing cost. The communications manager at oracle company clarified:

“So what we see is that smart contracts are replacing existing contracts for instance, we are specifically looking towards any existing digital agreements where all parties just inherit and don't trust each other. For example, one company's compliance department will have a copy and their billing department will have a copy too. They will have the same digital agreement and then if something needs to change about it, maybe some input happened, everyone will need to update their copy of the agreement. Therefore, we see smart contract replacing that type of scenario where everyone including government regulators could all just reference the same smart contract.”

In a complex environment, the smart contract may not fulfill all the terms of the contract unless it accesses information from a third party source for example in meteorological organization providing information about the weather to the farmers and the insurance company. This creates an opportunity for the meteorological organization to sell its data to the insurance company.
The IT Lawyer explains:

_We have areas that have been proposed to the smart contracts to deal with what are called “externalities”. Externalities is when everything can’t be dealt with inside the smart contract so you’ve got to actually go outside of the framework that called the blockchain and the smart contracts._

5.1.2. **Blockchain technology and IT systems**

Third parties that work with IoT, robotics and artificial intelligence can benefit largely from the emergence of smart contracts. For example, a person that is out jogging can have wearables that constantly track and send information to the blockchain. If that person has a health insurance, any type injury or health condition can be tracked and a smart contract can help the person by contacting a doctor when something out of the ordinary happens (Conference speaker).

Smart contracts require secure and trusted inputs from third parties like oracles. How do you trust that the information from an oracle is actually correct? The IT Lawyer explained:

_“The whole point of having an oracle is that it is a trusted third party and which can deliver accurate data. Now, what you are hoping is that there is some sort of security framework whether it is a SSL or VPN or whatever that connects the infrastructure with the blockchain, holding the smart contract and where the oracle is.”_

There is an increasing hype of blockchain technology by most experts in the Insurance and financial sectors about the opportunities of the technology itself. However, some experts claim that the technology is still in its early stages. The conference speaker clarified: _“There is a lot of talk about an amazing mission but the technology is not there yet and not many people have built blockchains and applications on it, so we need more of that and inspire people to start more of it.”_
One major problem with blockchain technology is that it requires large storage space as more blocks of transactions are added to it. The conference speaker clarified: “The whole blockchain becomes huge and if you want to run a node, you don’t want to download 250 Gb. You want the storage for your own and it becomes a problem.”

The development in the blockchain industry is moving over from Blockchain 2.0 to Blockchain 3.0, because of the challenges like speed and scalability in Blockchain 2.0. But there are still challenges as the conference speaker put it:

“[…] we don’t have an incredible source of information in this space like right now”

5.1.3. Insurance industry business model

According to the conference speaker, 2-3 billion people in the world lack traditional financial services. When these people have access to cryptocurrencies in their mobile phones, it creates an opportunity for the insurance industry.

Another thing smart contracts could do is to help with automatic payments. A smart contract can be created immediately after a person has selected the things he wants to be in his health insurance. If that person loses parts of his ability to work, an automatic payment could be made to that person when it is decided that he actually has lost parts of his ability to work. There is an opportunity for insurance companies to become more effective in this matter.

Home insurance is a simple product. The insurance industry can develop it further to sell more online. There could be options where the customer can choose what to include and to what level. Even life insurances can be bought online:

“Life insurance is a little easier because only if something happens to me in my life, that is, if I’ve deceased.”
Handling a damage claim is fast but it can become faster:

“[…] It's not lightning fast so the damage will be regulated by 22.20 tonight and you'll get an answer straight on.”

The continuous development of the insurance industry presents an increase of sales for online solutions such as auto insurances. The head of sales at an insurance company explains:

“Certainly, I see the car insurance increase online all the time. It is a simple product. It's easy to understand, it's easy to subscribe online. We can certainly develop it and make it even easier and more user-friendly absolutely. Such a product is very well suited for selling online.”

With the help of better technology, the insurance industry can shorten their work processes. As it is now, things are done manually:

“When they start the repair they might take away something from the front and it turns out that they have to replace more details that were impossible to see before. So it's not that they had done a mistake in the first evaluation because the evaluation was based on what they could see.”

5.1.4. Customer service

When there is a car accident with minor car damages, the insurance holder must first call the insurance company and then find a mechanic that can fix issues with the car. If the insurance company had stored the insurance policy in a blockchain, the smart contract could be triggered and an automatic system could find a mechanic for the insurance holder and notify him of where to go to get his car repaired and at what time. This would have saved the insurance holder time and he would have had a better experience.

Regarding the procedure of damage management, the insurance company follows certain ways in which it communicates with customers. Head of auto damages at an insurance company explains:
“We confirm always on the phone if the customer calls us. So confirm on the phone, but we will always send a letter to the customer. Letter by mail then, with confirmation of the whole. We also do that when the customer has made a digital notification. When the customer has chosen to communicate with us digitally, it becomes more natural that we also confirm digitally.”

5.1.5. Regulations

The insurance business is heavily regulated in the European Union which makes it difficult for an insurance company in one country to insure something in another country. The impracticality of managing damages in another country makes it uninteresting for insurance companies to offer their service in other countries in which they have no affiliates. One insurance representative said:

“I do not think Germany is interested in insuring property in Sweden. ‘Now we must go to Sweden and settle an injury there.’”

These challenges might be overcome with the emergence of new technology and regulations though.

There is a challenge of smart contracts regarding the technology and the law. Several authors state that there is a gap between the technology and the law. The IT Lawyer clarified:

“Well the difficulty with smart contracts is that they are actually very difficult to define from a legal perspective. That is the biggest conundrum or mystery out of all of these things because when you look at the various academic papers that have been published by going way back to Nick Szabo developed or proposed the concept of smarts contracts in 1996. The difficulty that you have is that there is a disconnect between the technology and the law.”
Blockchain technology makes records immutable. This raises issues when it comes to dealing with unacceptable terms of contract where there is no equal bargaining power between the contracting parties. The IT Lawyer clarified:

“You also have provisions where courts could say that provision is actually unlawful or unenforceable. We have what is called severability provisions. You also have provisions in certain jurisdictions in this country in particular but I know it under the European Union where a court can in effect rewrite aspects of the entire contract if they think it is unconscionable or unacceptable where there is no equal bargaining power. “

Related to the above is another scenario where the contract within the blockchain is totally unacceptable due to different parties involved at the time of negotiations. The IT Lawyer explains:

“It could and then you have to work out how you deal with; we have a concept called ‘void ab initio’, also means void from the beginning. If you have, a contract that is unconscionable or unacceptable because of different parties involved at the time of negotiating then there are positions where the court says ‘Now, we are going to seek this as void ab initio’ which means that anything that can be turned back, must be turned back.”

Regarding the issue of dispute resolution involving international jurisdiction where contracting parties of the smart contract are located in different countries. The IT Lawyer explains:

“Therefore, to deal with your issue where you might be in Europe and someone might be in Africa or in Australia, if you transact a commercial contract then there will be a nexus in Australia to that transaction and therefore I could bring you a proceeding. You then start getting about what is called Reciprocal Foreign Judgments legislation and it becomes very complex.”
There is an increasing debate on whether code in a smart contract is actually a legal contract. This issue is still contentious. The IT Lawyer clarifies:

“[...] Professor Ryan Lacey from Harvard University, even though I highly respect him, where he talks about ‘Code is law’. That is wrong. I repeat, ‘Code is law’. That is wrong. Law is law. Law is a set of rules that binds the relationships of the entities within that society. A set of rules binds the interrelationship of the entities within that society.”

There is a debate by some authors on whether the role of lawyers will be replaced by smart contracts (O’Shields, 2017). This is not going to happen soon. The communications Manager at the oracle company (New York) clarified:

“Well, as long as there’s a lot of the human factor, I don’t see the lawyers going out of the picture as far as regulation of the laws accepting smart contracts as well. Personally, I don’t see why not because they can be inspected by all parties, they can be altered and their state is their state. So, I mean in my personal opinion if it fits with the requirements of law as an agreement, it so happens to be a general agreement that exists on a decentralized system.”

Another challenge with blockchain technology is the lack of standards governing the development and implementation blockchain applications such as smart contracts. This raises fear among potential inventors. The IT Lawyer clarifies:

“The standards are still changing. In actual fact there are no standards. But you also have issues that there are new consensus algorithms, we don’t even have a finality yet on consensus”
5.2. Questionnaire

By using Contract Theory as the theoretical framework for this study, a questionnaire was created. The questionnaire can be found in Appendix B. A deductive content analysis was performed on the responses to come up with conclusions related the chosen theoretical framework. The seven themes that were identified from the theoretical framework and which were used to create the questions can be found in Table 6:

<table>
<thead>
<tr>
<th>Mutual assent</th>
<th>Contract cancellation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adequate consideration</td>
<td>Breaches</td>
</tr>
<tr>
<td>Establish capacity</td>
<td>Renegotiation</td>
</tr>
<tr>
<td>Legality</td>
<td></td>
</tr>
</tbody>
</table>

*Table 6: Theoretical framework themes*

Additionally, more questions were asked in the questionnaire in regard to the research questions of this study. These questions did not relate to the chosen theoretical framework but instead were related to the categories and themes in the inductive analysis following the exploratory interview study. These categories can be found in Table 7:

<table>
<thead>
<tr>
<th>Smart contract platform</th>
<th>Blockchain limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opportunities</td>
<td>Challenges</td>
</tr>
</tbody>
</table>

*Table 7: Theoretical framework themes*

From the deductive analysis on the questions related to the contract theory, it was found that some things are common between smart contracts and classic contracts and some things might not be applicable to smart contracts at all as of now.
5.2.1. Mutual assent

It is challenging to translate mutual assent from contract theory into code in smart contracts because the smart contract in itself does not necessarily need to contain an offer or acceptance. A smart contract can actually be just the result of an offer and an acceptance. An IT lawyer said:

“It is doubtful that smart contracts will start in this manner. A smart contract will reflect an existing standard set of terms initially”

But other respondents to the questionnaire said:

“The offer is inscribed in the smart contract code. Acceptance is relayed by accepting the terms of the Smart-Contract.”

and

“The offer is the code that will be executed by the contract code. The party writing the code and/or the beneficiary/recipient of value is offering a clear execution of this code. The acceptance is the activation of the smart contract program code.”

It is up to the developers of the smart contract to decide its functionality and how well it conforms to mutual assent, but most respondents agree that the offer and acceptance occur before the deployment of the smart contract.

5.2.2. Adequate consideration

How would a smart contract deal with a situation where subjective evaluation of quality of service against a services description is required in order to verify compliance? In other words, if a company promises a certain level of quality for a service, how can a smart contract assure the level of quality has been delivered before payment is done? Here the respondents gave many different answers. One said there is no way of doing it. One said
there should be a third party controlling the merchandise before payment is made and two of the respondents mentioned using oracles. The other ones could not give an answer.

5.2.3. Capacity

How can it be secured that either party in a smart contract has legal capacity to enter a contract? For example, if a minor is a party of a smart contract, how can this be handled after the smart contract has been activated? The simple answer to this is that it can be handled in a court of law according to some respondents, where the smart contract can be cancelled. Some respondents with technical backgrounds suggest that the smart contracts should contain functionality to deactivate a smart contract which rhymes well with the idea that a court of law is responsible for cancelling smart contract. But that also depends on how you code the smart contracts. Other solutions might be more effective. One respondent states:

“Depends on how you code it. Smart contracts can have different properties, like a central authority, or a DAO where delegates or shareholders vote on topics. You can also add a Freeze Account function.”

5.2.4. Legality

Are smart contracts legal contracts? The responses vary a lot. Some say yes, some say no and some say it depends. One of the respondents makes a good point:

“Smart contracts expand the definition of a legal contract. Whether they fit the legal definition of a valid contract in any given (let alone every) jurisdiction is up for debate. However, as self-executing code, they are essentially better than current contracts in that contracts only describe what the parties promise to do and how they will resolve disputes. Smart contracts execute these actions and are essentially irreversible.”
But what happens when the execution of the smart contract leads to actions that are incompatible with the law? Here the answers are more varying and some are contradicting. Some respondents say that it should be unenforceable or not be able to be executed but since smart contracts is just code, any programmer can write a smart contract and thus the events in the smart contract can be triggered. When that happens “There would be no recourse to law” as one respondent puts it. Another opinion is that “The law must comply since smart contacts are irreversible” and one respondents would even go to the extent of claiming:

“We should question if it matters and accept that the legacy law system will slowly become irrelevant.”

What if two parties agree on something and the smart contract they use does not correctly represent the agreement, how should the matter be resolved if the smart contract already has triggered some events? A lawyer responded: “lack of intention so not enforceable” which allows a court of law to invalidate the contract. Another respondent gave a more creative response:

“As in code, pre-agreed upon 3rd party that's specialized on the matter that'll handle the dispute”.

5.2.5. Contract cancellation

If all parties want to cancel a smart contract there are possibilities to do this using built-in functionality. Most respondents agree on using the self-destruct functionality of the smart contract when the parties want to cancel the contract:

“This can be programmed into the smart contract's logic before-hand (but not after). Where if some pre-determined addresses all agree to cancel the contract, they can do so to void it (Ethereum has a selfdestruct method).”

In the case of false data being used as input in a smart contract and the smart contract is executed, the contract needs to be corrected or invalidated in some way. There are
different ideas on how this could be done. One programmer responded that there should be precautions taken to avoid this situation to ever happen:

“To be completely safe, it would make sense for multiple requests to be made for the contract, where the actors that made the original request are not included for the others. Then only if those two answers agree will the contract be triggered.”

Another solution is to have built-in functionality in the smart contract so that the parties together can void the contract or by either party as specified in the smart contract:

“Anyone who is empowered to do so by the smart contract code as written. Sometimes no one. Sometimes only owner. Sometimes the party executing the contract (msg.sender) if this capacity is written into the code.”

If the case of fraudulent behavior they could turn to court of law to have the contract invalidated:

“If a contract is based on fraud, legal frameworks in every jurisdiction should declare it invalid.”

5.2.6. Breaches

Breaches are an important part of contract theory regarding classic contracts. There is however a difference when applied to smart contracts. Some respondents say that breaches in smart contracts are not an issue since the smart contracts are autonomous but that depends on how the smart contract is constructed according to one of the respondents:

“The well made smart contract hardly ever could be breached.”

How potential breaches are handled is also a matter of discussion as the respondents gave very different answers. Two of them said they do not know who would be responsible for dealing with a breach, one of them repeated that this situation is impossible, another said there should be new institutions. Three of them thought the law should handle it.
5.2.7. Renegotiation

Every once in a while, contracts are renegotiated. Smart contracts need to have this functionality too but how can this be achieved? Most respondents agree that there must be pre-programmed code that allows for a new contract to supersede the old one and this is most likely done by cancelling the old one and creating a new one:

“Classic contracts can have new contracts supersede them.

New signatures by the same parties invalidate old contract,
the same applies to smart contracts.”

5.2.8. Smart contract platform

It was clear that most respondents are more interested in the blockchain technology than in the Directed Acyclic Graph (DAG) technology. Only one respondent preferred DAG technology. Most of the respondents chose Ethereum as the platform best suited for smart contracts, but Cardano and Eos were also mentioned. A typical explanation to why Ethereum was selected as the best suited platform for smart contracts was:

“Developer adoption is already rapidly growing. Integration
with existing web technologies is fairly simple.”

5.2.9. Blockchain limitations

Even though the respondents chose blockchain before DAG technology, they were very well aware of the limitations of the blockchain technology. Many mentioned scalability and privacy as limitations and a few thought the main limitations were transaction speed, storage, security, user friendliness, lack of international standards and regulations. These limitations need to be overcome somehow and the solutions suggested were of different kinds. Some recommended secondary-layer solutions and other suggestions were consensus committees by organisations or states, and continued investments in research.
5.2.10. Opportunities

The blockchain technology brings many new opportunities for many different industries. For the insurance industry the usage of blockchains can result in increased transparency which makes the company more trustworthy since the data entered in the blockchain cannot be tampered with. By incorporating smart contracts in the payment processes, automatic payments can be made with less or no human interaction. Less human intervention could lead to more accurate data and this automation of processes reduces cost. The built-in trust in the blockchain makes it easier to protect against fraud.

Many respondents agree that there are big opportunities for tech companies to disrupt the insurance industry by offering new types of insurances like micro insurances and better integrations of technology. One respondent said:

“Smart contracts would allow tech companies to sell insurance with much less overhead than traditional insurance agreements.”

One respondent said that tech companies could also earn trust by offering their own insurances. Another said:

“massive opportunities for tech companies especially in software verification tools for smart contract deployments.”

This allows software companies to build products and services around smart contracts. They can for example create private blockchains and offer support around that as one respondent stated. They can even offer their own peer-to-peer insurance solutions. One suggestion was:

“peer to peer insurance could come into play especially in community insurance of association insurance. E.g. yacht clubs could start their own peer to peer insurance or auto clubs etc.”
Companies working with IoT and Artificial Intelligence have much to earn from working with the blockchain. One respondent said:

“[…] Blockchain/DAG in conjunction with AI, machine learning, and IoT -- all of which are natural partners for one another -- will completely reshape every industry.”

Other services that third-party companies can offer is consulting and auditing services.

5.2.11. Challenges

Most insurance companies make money by collecting as many insurance policies as possible and then be restrictive on pay-outs. Transparency can thus become a problem. As one respondent put it:

“Insurance companies (in the US) are often dishonest and make money from denying claims. Consumers need better transparency from them, such as why claims are denied and records.”

It is also difficult to get the specific data as input to the smart contracts in a safe and secure way. The lack of oracles will make it difficult to have trustless data and adapting quickly enough to the new competition from tech companies is a challenge for the insurance industry as one respondent stated:

“Adapting quickly enough as their industry is overrun by competitors using blockchain tech and decentralized insurance 'companies'. For those that embrace blockchain, the lack of worthwhile oracles for real world, trustless data will be a challenge for some time.”

Third parties offering services to the insurance industry and software industry will find it difficult to handle scams and criminal activity according to one of the respondents.
6. Analysis

Comparison and thoughts on how the results of this study conflicts with or agrees with the literature is presented. Ideas on solutions and where more research is needed are put forward.

6.1. Blockchain technology in the insurance industry

The insurance companies can benefit from automating payments using smart contracts. Contracts and claims stored on the blockchain can be validated through the network to make sure that valid claims are paid. Insurers can access information about their customers through one platform or system (PWC, 2017). The insurance conditions manager asserts that life insurance is an easier product to manage and sell online. Insurance policies such as life insurance can be automated so that in the event that the policyholder dies, the smart contract triggers payment to the beneficiaries. This, however, requires a trustworthy source of data. Why should you automate this process? It would lower costs, improve the time of processing claims and increase customer satisfaction. With blockchain technology, insurance companies can customize their products based on customer preference. For example, a customer could have the choice of selecting what to include in the policy stored in a smart contract.

Blockchain technology presents an opportunity to improve customer engagement. Crawford (2017) argues that blockchain can increase customer engagement and satisfaction since their information is digitally stored and verified through a single platform. The customers do not need to submit their documents more than once. Why change to innovative solutions with blockchain and smart contracts for customer engagement? This is because technology promises a new experience of business to customer interactions where customers will receive instant updates, for example regarding their loan applications and life insurance information. As the insurance sector
becomes more digitised, more businesses are looking for better ways of communicating with their customers. The head of auto damages at an insurance company asserts:

“When the customer has chosen to communicate with us digitally, it becomes more natural that we also confirm digitally.”

One of the biggest challenges with blockchain technology is how to make it scalable, that is, increase in size without introducing new problems. Benton and Radziwill (2017) notes that when blocks of transactions are added on the blockchain, each client verifies and records those blocks. As the blockchain expands in length, it requires more storage space as well as computing capability. The conference speaker also argues that the scalability is a problem:

“The whole blockchain becomes huge and if you want to run a node, you don’t want to download 250 Gb. You want the storage for your own and it becomes a problem”.

This means that in the future when a blockchain is more than for example 10 TB, very few individuals will run full nodes of the blockchain. This leads to a new problem. When only large organizations run full nodes, some of them come together and run a full-scale 51%-attack resulting in changes being made in the blockchain to the advantage of the attackers. This is a major security problem and the solutions are being worked on, but to our knowledge, there is no present solution for this problem.

From the analysis of the results, there was more emphasis on the lack of standards for shared and distributed systems. In fact, McKinsey&Company (2016) argues that the lack of standards and proven reference implementations shows the infancy of the technology. While the IT lawyer argues that, “The standards are still changing. Actually, there are no standards”, who would want to invest in a technology without governing standards? This raises a risk of implementing inefficient solutions if the industry standards are not established and defined. Insurance companies need to think about investment decisions wisely.
### 6.2. The law and smart contracts

There have been speculations that smart contracts entirely or in part might replace contract law. It is claimed that smart contracts will confront the juridical forces to deal with basic contract applications, but they will not replace contract law as they serve a different purpose according to Werbach and Cornell (2017).

According to the study by the Smart Contracts Alliance (2016), it is also argued that smart contracts will not replace the role of lawyers in the resolution of complex disputes. The lawyers will create a code that reduces the complex legal decisions needed to develop a workable commercial contract. Organisations will still employ traditional lawyers to negotiate the actual terms of the contract. The communications manager of an oracle company supports this argument where he emphasizes the importance of lawyers in verifying that the code complies with the law. Can smart contracts handle subjective issues such as quality of service? The answer is no. This justifies the need for lawyers and judges to decide on matters of subjective issues. However, there are solutions involving both smart contracts and humans that can help decide whether or not a service, or product, holds an acceptable level of quality. This can be achieved by using multisig decisions for example.

By common law, a contract can be terminated because of: frustration, impossibility, operation of the law, illegality or mistake or brought to end by cancellation (ab initio) (Norton Rose Fulbright, 2016). In such a scenario, Norton Rose Fulbright (2016) suggests that the contracting parties can seek the court to cancel the contract due to practicalities of the irreversible nature of the smart contract. This implies that the contract is void and what the parties had exchanged or transacted is returned to each party.

From the results, we understood that there is a knowledge gap in the IT industry around the legal validity of smart contracts. The IT lawyer argues that it is difficult to define smart contracts from the legal perspective. For instance, how does the code translate the concept of reasonableness? This involves a sense of judgement that is very difficult to turn into computer code. Norton Rose Fulbright (2016) argues that for smart contracts to be legal, they must have an offer and acceptance, consideration, intention to create legal
relations (capacity) and the legality of terms clearly defined. Some elements may not be possible to put in the coding of the contract.

It is not the purpose of contract law to enforce performance, but to handle cases where agreed upon performance has not been conducted. Smart contracts on the other hand ensures performance since they will autonomously carry out the tasks in the contract. This also means that there is no possibility of breach in smart contracts (Werbach and Cornell, 2017) which was supported by Savalyev (2017):

“A smart contract cannot be breached by a party to it”
(Savalyev, 2017, p. 130).

However, this is not always true though since smart contracts can be programmed to use multi-signature decision (multisig) for example, to have some manual control of the execution of the contract. That way, a third party may help decide whether a particular task in the smart contract should be performed or not, in case of some condition in the smart contract has been fulfilled. Multisig has its advantages and disadvantages too though. Using it in a smart contract means that smart contracts may not always be autonomous but on other hand, using multisig in smart contracts could result in more accurate and a higher number of intended outcomes.

Classic “contracts are deeply social tools as well as legal ones” (Levy, 2017, p 10). This means that contracts are often used as a tool for negotiation than in a court of law. How can this be done with smart contracts? The short answer is, it cannot. In code, things are either black or white. There is no grey zone for interpretation. Decisions in code are made by “if… then…”-statements and this means that either a condition is true, or it is false. Smart contracts are triggered when the programmed conditions are met so there are no juridical means to interrupt the execution of a smart contract. It can only be handled after execution but even then it might not be possible to undo the actions performed by the smart contract, for example, a smart contract that handles buying and selling of stocks (Werbach and Cornell, 2017).
According to the IT lawyer (personal communication, 2018, March 9), smart contracts need to be backed up by court cases when something out of the ordinary happens that is not regulated in the smart contract. This is because it is not possible today that all laws could be interpreted into computer code. The IT lawyer stated that code is not law, but what if it is law, what happens then? We believe that smart contracts initially will be used primarily as autonomous agents and as standards regarding smart contracts arise, the use of smart contracts as legal contracts will grow. In the beginning, however, there will be unexpected consequences from smart contracts that will highlight the logical errors and bugs as a result of the lack of standards and immature technology.

The core of contract law is that some agreements are legally binding which means if the agreement is breached, either party may take the other party to court. But it is up to the parties of the agreement to decide whether or not the agreement should be legally binding (Werbach and Cornell, 2017). The authors also argue that smart contracts are essentially different “because the digital code is not just a representation of the agreement; it is the agreement” (Werbach and Cornell, 2017, p. 344). Here the authors believe that the smart contract contain all the terms of the agreement which will not always be the case. Most of the questionnaire respondents argued that the agreement in most cases would take place outside of the smart contract, allowing it to be an autonomous agent that enforces the agreement.

6.3. Contract theory

Mutual assent
From the results we understood that there were different opinions on how smart contracts should be implemented. The IT lawyer stated that the offer and acceptance should be completed before the creation of the smart contract, but other respondents claimed the offer and acceptance should be stored within smart contract. There is nothing that prevents mutual assent to be expressed in code though (Werbach and Cornell, 2017), but according to O’Shields (2017) this is a tricky part of contract theory. On one hand, a website user must accept an offer, with a clear note of the terms, which will create a smart contract with certain functionality. On the other hand, if a smart contract would contain
an offer, it must be clear what the terms are before someone manually accepts the offer, otherwise the contract would be unenforceable.

This means that a smart contract must either have all the terms written in the smart contract or the terms must somehow be reachable from the smart contract. What would this “reachable” place be? Is it a pdf file located on a server somewhere? If that is the case, then the terms are not immutable. And how exactly would the terms be presented to the buying party if the offer is supposed to be in the smart contract? There are still no easy ways to state how a smart contract should be compiled and what it should contain and how it should be formed as there are no standards at the moment.

Another problem with smart contracts is that there might be logical errors in the code. For example, code that does not meet the legal conditions for mutual assent or code that commits to fraudulent behavior will be executed anyway as smart contracts are not smart enough to determine if the code mirrors the intended outcome of the agreement (Werbach & Cornell, 2017).

**Adequate consideration**

There is no consideration in smart contracts according to Werbach and Cornell (2017). The authors claim that there is nothing stopping someone from coding the smart contract to have no reciprocal promise, which is true of course since in code, anything can be programmed. But we must disagree here. If there is a lack of reciprocal promise in a smart contract and the seller does not notify the buyer of this but instead gives the appearance of the contract being an agreement with consideration, then this is fraudulent behaviour and thus renders the smart contract unenforceable. If the smart contract only refers to a promise of a gift, then of course there is no consideration and the smart contract is not a legally binding contract from contract theory point of view. So again, whether a smart contract is a legally binding contract or not depends on how it has been coded.
**Capacity**
According to contract theory, children, people with mental disorders and really intoxicated individuals do not have the capacity to sign a contract (Werbach and Cornell, 2017). But with smart contracts there is no way of testing the capacity of a signing party. If a child enters a smart contract, then its unenforceable but what if the actions of the smart contract already have been performed?

This brings up another very important issue with smart contracts. On a technical level, the parties involved are not actual people but cryptographic private keys (Werbach and Cornell, 2017). A private key represents an individual but there is no way to identify a person through that persons’ private key unless there is a ledger somewhere which binds a person to a private key. So how can a private key be tested to see if the holder of the private key does have capacity to “sign” smart contracts if there is no “identity ledger” available? Well, it cannot! Technologically we are not there yet because there are no standards or regulations for this. This is an issue that needs to be resolved to allow for a higher amount of enforceable legally binding smart contracts. There are already blockchains that work as identity platforms but to our knowledge none of which are valid as personal identification from a legal point of view.

**Legality**
In contract law, an unlawful contract cannot be enforced. But when it comes to smart contracts, there is no way to stop a task from being executed even if the court finds the terms of the smart contract unlawful. This is because smart contracts are self-enforcing (Hsiao, 2017). That is not entirely correct though. One way is to use the “self-destruct” functionality mentioned earlier. Another way is to use multisig where a third party can help cancel the smart contract if there is a built-in function for this.

**Contract cancellation**
Parties that are unsatisfied with the results of automated systems must be able to resort to the legal system. If the triggered actions of a smart contract turned out to be unintended, the legal system might disregard those actions (Murphy & Cooper, 2016).
Contract semantics

In classic contracts there are examples of text stating “the seller must deliver in a reasonable time” (Schwartz & Scott, 2003). Since smart contracts are autonomous programs, it is not possible to translate “reasonable” into code. It is a real challenge to translate contractual semantics to code (Norton Rose Fulbright, 2016). In the smart contracts, the amount of days or weeks in which the seller should deliver, must be stated. But here is something we as humans can adjust to. If the seller delivers the goods a day late, it might not make such a huge difference for the buyer who pays the invoice in full.

But if there is a smart contract involved and there is a breach clause in the contract stating that the seller should pay a breach fee for delivering the goods too late, then this might cause the smart contract to make a reduction in the transaction from the buyer to the seller, meaning that the seller receives a smaller payment. This could of course be a good thing, causing the seller to become better at upholding agreements but it might also cause new problems that might strain the relationship between the buyer and seller.

What if there was a delay in the shipping that was out of the sellers control? How could this be handled in a smart contract? Should multisig decision be used? Should the contract be renegotiated so there would be no fees or price reduction in payment? There are no standards as of now or recommendations on best practice on how to solve these types of issues as of now, it is only up to the programmers of smart contracts to decide what functionality the smart contracts will contain.

6.4. Opportunities

The results of the study show that smart contracts can offer an opportunity of automating processes of operations. Examples of this could be claim management and customer service. The communications manager of an oracle company argues that smart contracts can eliminate duplication of information stored at different departments of a company where for example many departments have copies of the same agreement. This can be solved by storing the digital agreement on the blockchain. The study by KPMG International (2017) shows that smart contracts can settle claims using coverage
information stored on the blockchain thus avoiding disputes and the need for extra reviews by insurance agents. This can lead to automation of claims payment thus eliminating duplication and need for input in some areas of operation.

The entire purpose of smart contracts is to trigger automatic events in case of activation. This automation replaces what was earlier manual processes, for example making a money transaction after the delivery of a product. Less human interaction means lower costs. In the case of auto insurances, automation can mean faster damage handling and the use of calculation robots might increase when processes are automated. With the help of AI even more automation would be possible in the insurance industry. But with new solutions come new problems. If processes are automated and something goes wrong, how would one detect the error? If something is wrong with the calculation robot and the automatic payments to policy holders results in too much money being paid out, what would be needed to detect this? Of course, there must be some type of control software that analyses the payments and alerts someone in the organisation when a payment is higher than a certain pre-decided sum. This opens new opportunities for IT-companies to build reporting software around smart contracts.

Furthermore, from the results it is understood that many new services are likely to emerge with smart contracts. IT companies will build and support private blockchains, offer consulting services and do auditing among other things. New third-party companies will come to life, offering multisig services, trusted sources, legal advice especially made for smart contracts, digital identity services for blockchains and other unthought-of services.

New insurance types will also emerge as automation, security and trust will be easier to accomplish and acquire. For example, pay-as-you-go micro insurance applications for cars (Vo, Mehedy, Mohania & Abebe, 2017) will be easier to handle with smart contracts. These micro insurances could for example be insurances that last for a day or just for a specific geographic area. Another example is delays. There are already insurance policies that can be bought for flight delays, that make automatic payments if a flight is delayed for more than a certain number of hours. These insurance policies reside within smart contracts on the blockchain.
Another opportunity for IT companies would be to create platforms for peer-to-peer insurances as the IT lawyer suggested. We had an idea that these IT companies can choose different types of business models where they can either sell the platform as a service to, for example yacht clubs or car clubs or they can start insurance companies themselves. In the option of selling the platform as a service, the clubs can come together over a certain geographic area and create their own insurance companies or DAO’s. Blockchain will take care of the storage of insurance policies, trust that the once saved information has not been tampered with and the automatic payments once a claim has been settled. Of course, a new insurance company must build an infrastructure around sales, claims handling, customer service and marketing which might be a challenge in itself but the possibilities are there. There are many examples where associations can come together and insure themselves instead on relying on big insurance companies that make profit by denying claims.

Peer-to-peer blockchains with DAO’s or DAC’s could replace the current system of corporations selling insurance policies as this digital construction could remove the profit from the industry as stated by a respondent to the questionnaire. In 2017 there were 20 insurance companies on the Forbes 500 list of most valued companies in the world and they are making huge amounts of profits every year (Sanchez, 2017). The more the insurance companies decline insurance claims from policy holders, the more profit the companies make. Peer-to-peer DAO’s or DAC’s using the blockchain technology or other types of decentralized technologies would quickly reduce the amount of profit the current insurance companies make when the general populations become aware of the new type of insurances that are using the blockchain technology. So, what is preventing digital social constructions such as DAO’s to start competing with the insurance companies?

That depends on what a DAO is and how it will be organized. There is an ongoing discussion in the world of blockchain where groups of people are trying to define how a DAO should be structured and used. During the analysis, some questions emerged: Who do people turn to for insurance claims in a peer-to-peer insurance network? Should they submit claims using a form on a website? Or is there an app you can download on your smartphone where you can get instant access to a voice recognizing AI? With automation comes less human contact, is this what insurance holders want when they are in need of
help? How does this affect the quality and how is this perceived by those in need of help? Is there a way to combine this new technology and still have the human contact when in need of help? These are all important questions that are related to the use of smart contracts and are subject for future research as they fall outside of the scope of this study.

We further believe that the opportunities and challenges for IT companies that want to start selling insurance policies are not to be equalled with those for the insurance companies. Insurance companies that are quick to adopt new technology has a bigger chance of staying ahead. One way of doing that is first to start learning and using a blockchain and start building smart contracts. This way they can learn what the IT companies are doing and start innovating new types of insurances before the IT companies learn about the insurance industry and start selling insurance policies online.

**Smart contract example use case**

The results implied that there are huge opportunities for IoT companies, data science companies and AI companies. During the analysis we thought of a scenario where smart contracts can integrate with other technologies:

A car hits another car in the rear leaving both cars slightly damaged and temporarily unusable. The man in the back car that ran into the other car has what is considered today a typical auto insurance. After the accident both cars pull over at the side and stop. The man in the back picks up his phone to call his insurance company and tell them what happened. After waiting in line for a few minutes he gives his statement to the insurance manager who gives the man an insurance number. The man must now call a tow truck to tow the car to a mechanic. The mechanic must first evaluate the damages and calculate the total cost of fixing the damages. Then this number is entered into the insurance company’s computer system. Now the insurance company must assess the situation and to keep the example simple we can say that there are two possible outcomes:

1. If the cost of fixing the damages is higher than the value of the car, the insurance company will deny the repair and a representative from the insurance company must contact the owner to tell him how much they will reimburse him for the car. After a negotiation the car owner accepts the offer and now has to buy a new car.
2. If the damage cost is much lower than the value of the car, the insurance company accepts the repair cost and a time is scheduled for repair. The owner of the car gets a phone call from the mechanic telling him that the car will be ready in two weeks.

The man in the other car on the other hand, has an insurance policy stored in a smart contract. His insurance company has a partner that equips cars with IoT devices to keep track of the whereabouts of the car as well as sensors that send information about damages when the car has been involved in an accident. When the car was hit in the rear, the cars computer registered the damages through the sensors and sent this information to the smart contract. The smart contract triggered several events at the same time:

- Sensory car data is sent to the closest mechanic.
- The insurance company AI customer service called the man in the car on the phone to learn about potential injuries and get a quick statement from the driver or passenger if the car was a self-driving car.
- A drone was sent to the place of the accident to register the accident and assess the situation. The drone is equipped with a camera and a speaker. At arrival the drone first looks for injured people and would alert the nearest hospital of location and number of injured people among other things. Then it registers the damages of the cars involved saving all videos and clips in a safe place in the cloud which is connected to the smart contract and insurance policy. If there are damages to other things, an assessment is made to call the fire department or police if needed. The drone also scans the policy holder in particular making sure that he has no injuries and if needed begins a conversation, learning what happened.
- A taxi or rental car is called to the place of the accident to take the insured person to his destination.
- A tow truck is called to the place of the accident.
- If the accident would have caused severe damages to the car, based on the data sent from the car sensors, an ambulance could be called to the location as well.

After the person has left the place of the accident, the tow truck takes the damaged car to a mechanic. This time the mechanic already has information about the parts that need
replacement and the report about repair costs has already been sent to the insurance company. The mechanic can manually add things to the report or change the work time to make the repair which replaces the previous report. The insurance calculation service, which is an AI, has done the calculations and made a decision. The car should be repaired and the car is towed to another mechanic that can finish the job faster. The policy holder gets a message that the car repairs will be finished within a week and is asked if he needs to have a rental car until the repairs are completed.

In this scenario, the use of smart contracts turns a damage claim into a completely different customer experience and it easy to identify the areas where IT companies can find opportunities:

- Insurance companies can use IoT services to track their insured vehicles and equip them with sensors of different kinds.
- IT companies can build API’s to allow car manufacturers built-in sensors in the cars to connect with insurance policies stored in smart contracts through oracles.
- AI services to communicate with the policy holders.
- Drone companies that offer on-demand services which can be signed through smart contracts. Drones do not need to be owned by the insurance companies.
- AI services to make insurance decisions based on IoT data.
- Telecom companies can provide extra bandwidth or special bands for IoT communication.
- IT companies can build API’s between insurance company blockchains, oracles, taxi companies, rental companies (drones, cars etc.), state institutions like fire department or police, hospitals, car mechanics, business systems and so on.
- IT companies can build private blockchains for different purposes.
6.5. Challenges

Transparency
It is our belief that one of the major challenges with transparency for the insurance companies is that data stored in a public blockchain allows anyone to see why a claim has been denied. This would be risky for an insurance company that make more money the more claims they deny. But if other insurance companies start being more transparent, those who do not, will have a hard time competing with those who do. There is another aspect of transparency. In the EU, the GDPR privacy law can cause problems when smart contracts are storing personal information and if this information is unencrypted it is transparent to all viewers. The immutability of the blockchain takes the problem to another level. Once a transaction has been recorded and verified, it cannot be changed by anyone.

Legal issues
Benton and Radziwill (2017) argue that the existence of the transaction in the blockchain may not guarantee a true representation of the interaction between two parties. So, what happens if one of the parties disagrees with the outcome of the agreement and yet the terms cannot be changed? Now, if both parties agree to seek mediation, that is when the court of law intervenes. The IT lawyer clarifies:

“You also have provisions where courts could say that provision is actually unlawful or unenforceable”.

This implies that the court could advise both parties to rewrite those aspects of the contract that are questionable. However, to implement such changes in the code that resides on the blockchain is difficult. Another solution would be to cancel the contract and create a new one. This can be done using the ‘self-destruct’ functionality on the Ethereum platform for example.

Human resource issues
Insurance companies that want to adopt the blockchain technology and learn about how smart contracts can help them automate processes, might have difficulties in hiring people who can build the solutions. To our knowledge there are no academic programs
specialized in blockchain and smart contract programming. There are online courses and some universities offer a few courses, but we believe it would be hard to find experienced smart contract programmers that are willing to start working at insurance companies. The solution to this could be to partner with an IT company specialized in smart contracts that would build the solutions for the insurance company.

Trustworthy data
In theory it is easy to get data from one end to another, but in practise it can be difficult to get the specific data as input to the smart contracts in a safe and secure way as one respondent from the questionnaire stated. We think that the lack of oracles and country specific oracle nodes will make it difficult to acquire trusted data. Trusted data can only be fetched from trusted sources and these trusted sources might be difficult to find and connect to. For example, if there is a life insurance smart contract that pays a certain amount of money to a selected beneficiary in case of the policy holder deceases in an accident, then there must be a way to check whether or not the policy holder has deceased and this data must come from a trustworthy source. If there is no trusted source that can deliver this data, then there can be no service of this kind. This means that the government institutions must be able to supply this kind of data when asked for. This in turn means that governments and state institutions should play a big part in the smart contract ecosystem. If there are no API’s to government records, then the number of trusted sources will probably be low, so this puts some pressure on the government institutions as well, if the government have goals to be in the forefront of technology.

Barriers
For IT companies that want to offer insurance services there might be a big barrier to climb when they need to learn about and deal with end customers, regulations and disputes. There are laws that regulate the insurance industry and it is a multidimensional apparatus. There are many challenges to overcome and if blockchain technology is going to be used, there will be more things to take into account as the use of blockchain technology might not always be the best solution. It will also be a challenge to know when to use blockchain technology and when other solutions might be better as one questionnaire respondent stated.
**Fees**

The blockchain built-in costs for mining is also a challenge because the mining fees are related to the cryptocurrency price. When it has a high value then the miners make more money for mining and when the value of the cryptocurrency is low the profit is low. When the monthly profit for mining is lower than the monthly electricity cost, then the miners will stop mining. If this happens there might be too few miners that are willing to continue mining in relation to the number of blocks waiting to be added to the blockchain and this can create increased latencies for the blockchain.

There is another problem with having a cryptocurrency with a high currency value. The blockchain mining fees are related to its value meaning that the fees increase as the price of the cryptocurrency goes up. For example, when one Bitcoin was valued over 15,000 USD, the fee for a transaction could be more expensive than the product or service being bought. Nobody would be interested in buying a coffee for three USD and pay 50 USD to complete the transaction, which was the case in December 2017 (BitInfoCharts, 2018).

The blockchain technology has some issues with mining costs as well as the cryptocurrency value. A cryptocurrency that is future proof should not be dependent on the value of the cryptocurrency in itself but should instead be valued for its built-in value generating properties. We believe that a cryptocurrency that can be used on a global scale must not be a currency one can speculate in. The mining and transaction costs must be minimal for it to be worth using a cryptocurrency.

As children are learning about using technology from a very early age, we predict that in the future all types of services will be available online and buying a service will be as easy as clicking a buy-button. The work processes of a service will be automated and smart contracts will most likely be the machines that produce the result. That is why insurance companies need to start using the blockchain technology. Otherwise they might end up like Kodak, doing too little and too late until the day comes when the company is no more.
7. Conclusion

Summary of the study and answers to the research questions.

The purpose of this study was to understand how insurance companies can adapt to the changes that smart contracts might bring. The blockchain technology is fairly young and has much potential in changing the work processes in many industries. With the development of smart contracts, there are many opportunities for companies to innovate themselves. The entire insurance industry could with the help of smart contracts, shorten the time frame for claims, make customer experience better, automate payments, eliminate duplication of reports and avoid disputes. For example, fraudulent behavior is a main issue and costs the insurance industry vast amounts of money every year. With the help of blockchain technology, the whole insurance industry can work together to better protect themselves from fraud.

The increased use of smart contracts will most likely present new types of services like consulting, auditing around blockchain and smart contracts in general. Other examples could be trusted sources, multisig services, legal advice and digital identity services. The birth of these new types of services and innovations around blockchain are likely to lead to new types of insurance types like pay-as-you-go micro insurances for example. The blockchain technology together with smart contracts can even lead to more disruptive ideas like peer-to-peer insurances.

There are many opportunities for the insurance companies to reinvent themselves and thus becoming more effective in their work processes. By introducing smart contracts in selected work processes, they can shorten the time frame for damage claims and make things easier for the customers when the customer needs to get in touch with customer service for example. Fraudulent behavior from certain groups is a main issue and costs the insurance industry vast amounts of money every year. With the help of blockchain technology, the whole insurance industry can work together to protect themselves from fraud.
There are however some challenges the insurance companies will face while adopting the new technology. Some of their work processes need a total overhaul when the manual work will be replaced by automated events. The shift to blockchain and smart contracts can result in reorganizations of different work processes, routines and people.

Rome was not built in a day and the shift to using blockchain will not be very swift either, but if the insurance companies start adapting their current processes to this new revolutionary technology now, they can stay ahead of the new competition instead of risking disruption from those who can adopt it faster.

### 7.1. Limitations

The aim with this study was to gather information about opportunities and challenges for the insurance industry using smart contracts. The goal was to meet with many different actors from different sectors but due to lack of interest from many of the potential interview candidates, it was only possible to arrange for interviews with one actor per sector. This limited the study in the sense that the responses to the interview questions might not have been typical for the sector.

The respondents from the insurance sector were not very informed about the blockchain technology and thus there was no discussion about blockchain during the interview. We had hoped there would be a discussion on the impact of blockchain on the insurance company’s business processes, but that did not happen which affected the results presented and thus limited our study. It was also difficult to find more potential interview candidates due to the time frame of this study.

The questionnaire only had ten respondents, which might have limited the amount of possible opportunities and challenges listed in this study. It was quite obvious that the number of respondents of the questionnaire that had knowledge and experience with contract theory was low as some answers to the questions about contract theory were either unanswered or irrelevant. This could have limited the results in the sense that more
ideas would have been explored if there were more respondents with better knowledge of contract theory.
8. Discussion

This chapter describes the discussions around the results, selected methods, research implications and recommendations for future research on the subject.

The aim of this study was to find out how insurance companies can adapt to the changes that smart contracts bring. In the next subsections, noteworthy discussions are listed and explained.

8.1. Results discussion

Many results in this study were both as expected and surprising. The knowledge of the blockchain technology in the insurance industry is limited. The reason for this could be that the blockchain technology is fairly young and there are few applications using this technology, so this was expected. What was surprising though was that they were not in a hurry to learn and understand how this technology could affect their future business and business models. This could be because there are no current immediate threats to their ways of doing business at the moment or at least they are not aware of them.

Another surprising finding from the interviews was the importance of politics and regulations. The politicians make the decisions and create the laws. The development of smart contracts and its use is dependent on the laws governing contracts so it was something we were aware of but which we did not understand the impact of.

Currently, there is a hype around blockchain in the media but for all the wrong reasons. Media writes about Bitcoin and cryptocurrency speculation but blockchain is so much more. Blockchains and smart contracts can solve many problems and shorten work processes making organizations more effective, but the extent of this surprised us. We believe that the people working with this are pioneers and in the near future we will see
many real applications on the market affecting many more. This can be explained by the core technical properties within blockchain resulting in its built-in trust and immutability.

The blockchain technology and smart contracts both have their limitations and solutions are being worked on, resulting in many new discoveries in a short period of time. This means that the problems and limitations of today, will probably be solved in the near future. It is hard to keep up with the progress and difficult to understand where to start, but with the help of standards, it will probably become easier to identify the opportunities that lie ahead. This is important because the lack of standards in the smart contract industry means that any company can write smart contracts any way they want. After the introduction of standards, there is a possibility that many smart contracts will not be backwards compatible and new versions would need to be created.

The introduction of standards would result in an easier comprehension of how to develop third party services which will allow IT companies to more easily identify the opportunities. Smart contract standards and the practice of contract law regarding smart contracts will most likely make it easier to know how to construct smart contracts in the future.

8.2. Methods discussion

Before we started this study, we searched for books and peer-reviewed articles about smart contracts and case studies on insurance companies using the blockchain technology. This search resulted in a very limited number of books and articles and we realised that if we were to contribute to the research in this area we needed to acquire primary data from the insurance industry. That is how we decided to do this interview study. The qualitative content analyses made on the interview transcripts further made us understand that the knowledge of contract theory and its application on smart contracts was also limited, driving us to create the questionnaire with in-depth questions on particularly contract theory. We thought this was the best way to explore the subject in detail for these reasons.
Because of the lack of information on the subject and lack of juridical knowledge in the IT companies, a quantitative survey around smart contracts and contract theory would be a bad idea. We could not perform a case study either because we were unable to find an insurance company that had already started using the blockchain technology with smart contracts.

The review of literature helped in broadening understanding of smart contracts from different perspectives. From this knowledge, we were able to investigate how the different aspects of contract theory relate to the application of smart contracts. The existing literature helped us to compare with the findings thus meeting the purpose of the study.

We wanted to understand how insurance companies could adapt to the changes brought by using smart contracts through exploring the opportunities and challenges of using blockchain technology and smart contracts.

One of the weaknesses of the chosen qualitative method was the restrictive aspect of the theoretical framework whereby some respondents may not have expressed their views because of their limited knowledge about contract theory as applied to smart contracts and blockchain technology.

### 8.3. Implications for research

The results of this study point out the importance of standards and regulations especially around legally binding smart contracts as well as the importance of a mature ecosystem of third party services.

This study makes a difference for:

- Insurance companies that want to learn more about or start using the blockchain technology.
- IT companies that are interested in finding new opportunities within the realm of blockchain technology in general and smart contracts in particular.
- Law firms that want to understand the impact of smart contracts.

For insurance companies it means that they could learn about what problems smart contracts can solve, how it can make the organization more effective and what could happen if they do not adopt the technology while competitors and others do. IT companies that get involved in this technology might discover new ways of finding customers or do business. The IT industry is a very innovative industry and IT companies may find gaps to fill around smart contract services or even in the insurance industry.

In the academic world there has been a debate whether or not smart contracts can replace the need for lawyers and how it might disrupt the industry (Lauslahti, Mattila & Seppälä, 2017; Sherborne, 2017, Smart Contracts Alliance 2016). Law firms that are interested in learning more about this can benefit from reading this study to understand how contract laws apply to smart contracts and how it affects the judicial industry and the courts.

Other organizations that might find this study interesting are:

- Government institutions
- Students that are generally interested in smart contracts.

### 8.4. Implications for practice

The authors of this study believe that the results could be useful for insurance companies that want to learn more about the benefits and challenges of smart contracts, smart contract programmers that would like to know more about what should be included in legally binding smart contracts and IT companies that are interested in the opportunities the blockchain technology offers.

There are many aspects of blockchain technology and smart contracts. There has been some research on the subjects, but there are very few use cases where smart contracts have been utilized by insurance companies. It is important for the insurance companies to be up-to-date with the progress of this technology, look further into the opportunities
it offers and start researching how the technology can benefit the insurance companies and their policy holder, but at the same time it is also important to not jump head-first into the new opportunities because of three main reasons:

1. The technology is changing fast. The blockchain technology is good but has its limitations. As new platforms are developed, some of the problems with the limitations are solved, but this DLT technology still has issues that are difficult to get around. For example, it is still serial as compared to parallel. Blocks in the blockchain are added one at a time in a single line of blocks. The more a blockchain is used, the more transactions would be placed in queue waiting to be added to a block and placed in the blockchain because the blocks are only added every X minute, where X is different from blockchain to blockchain. This increases the latency. There are solutions such as the Lightning Network (Lightning Network, 2018) but this involves placing transactions outside of the blockchain which in turn causes new problems. When transactions are placed outside of the blockchain, the immutability is taken away. There are other DLT technologies that are not based on blocks being added serially in a chain, but instead transactions are added to a graph of previous transactions. An example of this is the cryptocurrency IOTA that uses an algorithm called Tangle which is based on the DLT technology Directed Acyclic Graphs (DAG) (Popov, 2017).

2. There are no standards for how smart contracts should be built and what functionality it should contain, even if the smart contract is a legally binding contract.

3. The ecosystem for third party services is not mature yet. There are few oracles available, few trustworthy sources with public API’s and it is not yet easy to find companies offer services around smart contracts in general.

Checklist for insurance companies that want to start using blockchain technology:

1. Start learning where the processes need to be shortened
2. Start learning where the processes could to be shortened with the blockchain technology and smart contracts.
3. Start learning how to use the technology in practice.
4. Start building a private blockchain and use it to change and improve work processes. This way the company would learn how to do things in a way that works best for the company but also learn about what third party services are needed to get things to work as intended and maximize efficiency as well as understand the maturity of the needed ecosystem of third party services.

5. Develop a strategy for implementing blockchain technology and smart contracts within the insurance company and then connect to other third parties.

**Smart contracts and the law**

It is important that both parties understand the contents and results of smart contracts and the creators of the smart contracts need to know about the law as well. A smart contract programmer must do his best to make sure that the smart contract complies with the law and the only way to do this is with the help of a lawyer.

**8.5. Future research**

This study identified several areas that would be interesting to research further. These were:

1. In order to expand this research, future research should include more interview candidates from more insurance companies to get a better understanding of the working processes in more departments in the insurance industry. It would also be beneficial to use more respondents with knowledge of contract law to answer questions on how contract theory can be applied to smart contracts.

2. Throughout this study it was mentioned that the lack of standards for smart contract contents made it difficult to plan for the deployment and use of smart contracts. It would be helpful to understand how standards would add to the ease of creating and use of smart contracts.

3. This study has not addressed issues that arise from the application of smart contracts in a multi-jurisdiction setting. Research could explore the application of smart contracts in multi-jurisdiction setting.
4. Research on how contract theory could be used in practice during the creation of legally binding smart contracts, would be beneficial.

5. Another important question that was found in this study was that around fraud. How can fraud be prevented in smart contracts?

6. Research could explore the differences between using smart contracts on a blockchain and other DLT technologies such as Directed Acyclic Graphs for example.

7. An in-depth exploration of the ecosystem of third party software and services around smart contracts would be very helpful.

8. This study touched upon the ethical and legal issues regarding privacy, but we believe there is more room for future research in this area. It would be helpful to further research the questions related to smart contracts and laws on privacy.
9. Reference list


10. Appendix A- Interview guide

Interview questions

1. Could you please tell us a little about yourself and what you do? (name, age, city, company name, role, number of years at the company)
2. When did you start working with the blockchain technology?
3. What services do you offer?
4. Why did you start with this?

Blockchain

5. How are you using the blockchain technology?
6. What are the best things about the technology?
7. What are the worst things?
8. What do you think this can lead to? How will the blockchain develop?
9. What are the new intermediaries in the blockchain value chain?
10. What are the internet of things applications based on blockchain?
11. How does AI fit with the Blockchain technology?
12. What are the challenges of implementing blockchain applications?
13. How will blockchain technology affect the role of agents and brokers in the insurance industry?
14. How will blockchain technology affect contractual practices?

Smart Contracts

15. What are Smart Contracts?
16. What are they for?
17. What are the opportunities of using smart contracts?
18. What are the challenges of implementing smart contracts?
19. How do you think smart contracts can disrupt businesses?
Questions to The IT Lawyer

Our intro

1. Tell us a little about yourself (background)
2. What are you working with right now?

Legal issues

3. What can you tell us about general contract law?
4. What could be the legal issues with digital contracts as they are today?
5. How are issues with digital contracts settled today?
6. Tell us more about the legal aspect of smart contracts.
7. How do you propose issues regarding smart contracts to be resolved?
8. GDPR (*General Data Protection Regulation*)?
9. How can tech companies that work with storing data in the blockchain also fulfill the GDPR?
10. How can contract law be applied to smart contracts? (key concepts)
11. Tell us more about the phases of contract law in relation to smart contracts such as:
   - Formation of the contract
   - Performance of the contract
   - Breach of contract
12. What changes will be created in the contract law as result of using smart contracts?
13. How will DAO's and DAC's be considered from a legal point of view? Like a company?

Risks
Blockchain
Smart Contracts
Oracles.
Opportunities
Tech companies
Communities (Example: peer-to-peer insurance through a DAO/DAC)
3rd parties (Example: investigators for fraud, IOT and AI tech companies (drones with cameras and other types of scanners))

Questions to Communications Manager, at an oracle company

1. What problems does Chainlink solve?
2. Why should Smart Contracts use polling from an oracle?
3. Explain oracle bidding. Why not random selection?
4. How will Chainlink network improve the creation and usage of smart contracts?
5. How would Chainlink connect with trustworthy sources? Whose responsibility is that? (different markets and countries)
6. How does a company or organization that run a Chainlink node make money?
7. What other incentives but money are there to run a node? (costs like electricity, hardware, workforce etc.)
8. Would not it be cheaper and better for the users of Smart Contracts to avoid intermediary oracles and get information straight from the source?
9. Is it possible to use Smart Contracts without oracles?
10. What are your predictions on Smart Contracts using IOT, Big Data and AI?
11. What are the business opportunities of Smart Contracts? (insurance industry and others)

Intervjufrågor försäkringsbolag

1. Hur går det till när en försäljning av en försäkring sker?
2. Hur ser processen ut?
3. Vilka tekniska hjälpmedel används för att sälja försäkringar?
4. Hur lagras information?
5. Hur delas informationen med andra försäkringsbolag?
6. Vilka typer av tredjepartsföretag finns det?
7. Var kommer försäkringsmäklarna in i bilden?
8. Vilken roll har de och varför klarar inte försäkringsbolagen själva av det jobbet?
9. Vilka förbättringar kan göras i samband med försäljningen?
10. Hur tas villkoren fram för en försäkring?
11. Anpassas de löpande efter skadestatistiken?
12. Hur påverkar utbetalningarna försäkringspremien? Kan man välja utbetalningsnivå på livsförsäkring eller annan försäkring?
13. Vilka är riskerna med att ta fram villkor?
14. Vad gör ni för att förenkla förståelsen av villkoren?
15. Vad händer när en skada sker?
16. Vilka förbättringar kan göras i samband med skadhantering?

Insurance brokers and agents

17. What are the roles of insurance brokers and agents?
18. How can automation of their roles be impacted for example if claim processing is automated by using smart contracts?
Appendix B – Questionnaire questions

Mutual assent
1. What is the offer and what is the acceptance in a Smart Contract?
2. When does the offer and acceptance of the agreement occur?

Adequate consideration
3. How would a Smart contract deal with a situation where subjective evaluation of quality of service against a services description is required in order to verify compliance?

Establish capacity
4. What if one party did not have the legal capacity to enter into the smart contracts for example one party being a minor, how can this be handled after the Smart Contract has been activated?

Legality
5. Are Smart Contracts valid legal contracts? Why/why not?
6. What happens if the output of the smart contract is incompatible with the law?
7. If the code does not reflect what the parties agreed on to be in their contract. How is this addressed?
8. How do Smart Contract coders know which law has precedence over the other?

General questions
9. How are breaches handled for the different categories?
10. How do you make a Smart Contract void (get cancelled)?
11. Classic contracts can be renegotiated. How is this done in practice with Smart Contracts that are already activated in a blockchain?
12. Who will be responsible for handling breaches?
13. Who has the power to cancel a Smart Contract?
14. What if data used as input to a Smart Contract has been falsified. How can this be corrected? What legal implications does this have to the parties? Is this handled by a clause in the contract and what if there is no such clause?

Opportunities and Challenges
15. What opportunities and challenges do you see for insurance companies?
16. What opportunities and challenges do you see for tech companies that might want to sell insurances online?
17. What opportunities and challenges do you see for existing third party companies?
18. What opportunities and challenges do you see for new third party companies?

Blockchain

19. Which Distributed Ledger Technology do you prefer (Blockchain/Directed Acyclic Graph)?
20. Which technology is best suited for Smart Contracts? Why?
21. What are the limitations of the blockchain technology?
22. How should these limitations be overcome?

Link to questionnaire responses:
https://docs.google.com/spreadsheets/d/135w_dcaijOM_le5lUZEBrBeQL3g2OmH2xRFj7_eOlko/edit?usp=sharing
Appendix C – Categories from the interview transcripts

Interview 1: Conference speaker

<table>
<thead>
<tr>
<th>Category</th>
<th>Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blockchain technology (20+)</td>
<td>Blockchain Technology and IT systems</td>
</tr>
<tr>
<td>Challenge (1)</td>
<td></td>
</tr>
<tr>
<td>Cryptocurrency (13)</td>
<td></td>
</tr>
<tr>
<td>Currency (3)</td>
<td></td>
</tr>
<tr>
<td>Digital asset</td>
<td></td>
</tr>
<tr>
<td>Digital currency</td>
<td></td>
</tr>
<tr>
<td>DLT (2)</td>
<td></td>
</tr>
<tr>
<td>Future (7)</td>
<td></td>
</tr>
<tr>
<td>Smart Contracts (4)</td>
<td></td>
</tr>
<tr>
<td>Contract Theory (1)</td>
<td>Regulations</td>
</tr>
<tr>
<td>Crime prevention (1)</td>
<td></td>
</tr>
<tr>
<td>Globalization</td>
<td></td>
</tr>
<tr>
<td>Law (4)</td>
<td></td>
</tr>
<tr>
<td>Opportunity (2)</td>
<td></td>
</tr>
<tr>
<td>Personal (2)</td>
<td></td>
</tr>
<tr>
<td>Politics (7)</td>
<td></td>
</tr>
<tr>
<td>Disruption (8)</td>
<td>Third parties</td>
</tr>
<tr>
<td>Business idea (14)</td>
<td></td>
</tr>
<tr>
<td>Third party (11)</td>
<td></td>
</tr>
</tbody>
</table>

Interview 2: The IT Lawyer

<table>
<thead>
<tr>
<th>Category</th>
<th>Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blockchain (3)</td>
<td>Blockchain Technology and IT systems</td>
</tr>
<tr>
<td>Ethereum issues (1)</td>
<td></td>
</tr>
<tr>
<td>Oracle functionality (2)</td>
<td></td>
</tr>
<tr>
<td>Organization (1)</td>
<td></td>
</tr>
<tr>
<td>Smart contract functionality (3)</td>
<td></td>
</tr>
<tr>
<td>Smart contracts (3)</td>
<td></td>
</tr>
<tr>
<td>Insurance standards and legislation</td>
<td>Regulations</td>
</tr>
<tr>
<td>Legislations (10)</td>
<td></td>
</tr>
<tr>
<td>Privacy (1)</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Theme</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Blockchain (1)</td>
<td>Blockchain Technology and IT systems</td>
</tr>
<tr>
<td>Chainlink advantage (1)</td>
<td></td>
</tr>
<tr>
<td>Chainlink functionality (2)</td>
<td></td>
</tr>
<tr>
<td>Ethereum cost (1)</td>
<td></td>
</tr>
<tr>
<td>Oracle advantage (1)</td>
<td></td>
</tr>
<tr>
<td>Oracle functionality (8)</td>
<td></td>
</tr>
<tr>
<td>Oracle requirement (1)</td>
<td></td>
</tr>
<tr>
<td>Research and development</td>
<td></td>
</tr>
<tr>
<td>Smart contracts (2)</td>
<td></td>
</tr>
<tr>
<td>Smart Contracts cost (2)</td>
<td></td>
</tr>
<tr>
<td>Smart contracts functionality (2)</td>
<td></td>
</tr>
<tr>
<td>Node operator profit (1)</td>
<td>Third parties</td>
</tr>
<tr>
<td>Oracle cost (1)</td>
<td></td>
</tr>
<tr>
<td>Oracle payment (1)</td>
<td></td>
</tr>
<tr>
<td>Trusted sources (1)</td>
<td></td>
</tr>
</tbody>
</table>

Interview 4: Head of sales, Conditions manager and Head of auto damages, (at an Insurance Company).

<table>
<thead>
<tr>
<th>Category</th>
<th>Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreements (6)</td>
<td>Regulations</td>
</tr>
<tr>
<td>Authority</td>
<td></td>
</tr>
<tr>
<td>Laws (19)</td>
<td></td>
</tr>
<tr>
<td>Insurance terms 10</td>
<td></td>
</tr>
<tr>
<td>Data ownership (1)</td>
<td></td>
</tr>
<tr>
<td>Customer data (5)</td>
<td></td>
</tr>
<tr>
<td>Blockchain technology (2)</td>
<td>Blockchain technology and IT systems</td>
</tr>
<tr>
<td>Data communication (2)</td>
<td></td>
</tr>
<tr>
<td>IT (15)</td>
<td></td>
</tr>
<tr>
<td>New technology (1)</td>
<td></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Smart contracts (4)</td>
<td></td>
</tr>
<tr>
<td>Technical improvements (6)</td>
<td></td>
</tr>
<tr>
<td>Automation (4)</td>
<td></td>
</tr>
<tr>
<td>DLT (4)</td>
<td></td>
</tr>
<tr>
<td>Digital information (3)</td>
<td></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Background (4)</td>
<td>Insurance industry business model</td>
</tr>
<tr>
<td>Business model (21)</td>
<td></td>
</tr>
<tr>
<td>Business process (5)</td>
<td></td>
</tr>
<tr>
<td>Damage management (18)</td>
<td></td>
</tr>
<tr>
<td>Claims (5)</td>
<td></td>
</tr>
<tr>
<td>Disagreement</td>
<td></td>
</tr>
<tr>
<td>Insurance company (4)</td>
<td></td>
</tr>
<tr>
<td>Operations (7)</td>
<td></td>
</tr>
<tr>
<td>Price calculation (7)</td>
<td></td>
</tr>
<tr>
<td>Price evaluation (3)</td>
<td></td>
</tr>
<tr>
<td>Statistics (3)</td>
<td></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Business opportunity (6)</td>
<td>Third parties</td>
</tr>
<tr>
<td>Competition</td>
<td></td>
</tr>
<tr>
<td>Ethics (5)</td>
<td></td>
</tr>
<tr>
<td>Future opportunity (1)</td>
<td></td>
</tr>
<tr>
<td>Risk assessment (1)</td>
<td></td>
</tr>
<tr>
<td>Third party (21)</td>
<td></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Communication (8)</td>
<td>Customer service</td>
</tr>
<tr>
<td>Customer service (10)</td>
<td></td>
</tr>
<tr>
<td>Human perspective (2)</td>
<td></td>
</tr>
<tr>
<td>Understanding (2)</td>
<td></td>
</tr>
</tbody>
</table>
Appendix D – Transcripts

You can access the transcripts from the interviews below.

Link to folder with interview transcripts:
https://drive.google.com/drive/folders/1n1DK_3hCOLkJdpjMp80BcqUlOvn2DgZY?usp=sharing