UNIVERSITY OF LJUBLJANA
SCHOOL OF ECONOMICS AND BUSINESS

MASTER'S THESIS

AN ANALYSIS OF BLOCKCHAIN INNOVATION IN THE INSURANCE INDUSTRY

Ljubljana, October 2022 NIKOLIJA VUJIČIĆ

AUTHORSHIP STATEMENT

The undersigned Nikolija Vujičić, a student at the University of Ljubljana, School of Economics and Business, (hereafter: SEB LU), author of this written final work of studies with the title An analysis of blockchain innovation in the insurance industry, prepared under supervision of Aleš Groznik.

D E C L A R E

1. this written final work of studies to be based on the results of my own research;

2. the printed form of this written final work of studies to be identical to its electronic form;

3. the text of this written final work of studies to be language-edited and technically in adherence with the SEB LU's Technical Guidelines for Written Works, which means that I cited and / or quoted works and opinions of other authors in this written final work of studies in accordance with the SEB LU's Technical Guidelines for Written Works;

4. to be aware of the fact that plagiarism (in written or graphical form) is a criminal offence and can be prosecuted in accordance with the Criminal Code of the Republic of Slovenia;

5. to be aware of the consequences a proven plagiarism charge based on the this written final work could have for my status at the SEB LU in accordance with the relevant SEB LU Rules;

6. to have obtained all the necessary permits to use the data and works of other authors which are (in written or graphical form) referred to in this written final work of studies and to have clearly marked them;

7. to have acted in accordance with ethical principles during the preparation of this written final work of studies and to have, where necessary, obtained permission of the Ethics Committee;

8. my consent to use the electronic form of this written final work of studies for the detection of content similarity with other written works, using similarity detection software that is connected with the SEB LU Study Information System;

9. to transfer to the University of Ljubljana free of charge, non-exclusively, geographically and time-wise unlimited the right of saving this written final work of studies in the electronic form, the right of its reproduction, as well as the right of making this written final work of studies available to the public on the World Wide Web via the Repository of the University of Ljubljana;

10. my consent to publication of my personal data that are included in this written final work of studies and in this declaration, when this written final work of studies is published.

Ljubljana, _____ Author's signature: _____

(October / 02 / 2022)

TABLE OF CONTENTS

INTRODUCTION **1**

1 BLOCKCHAIN **2**

1.1 Introduction to the blockchain **2**

1.2 Concensus mechanism **7**

1.3 Distributed ledger technology **9**

1.4 Typologies of blockchain **11**

1.5 Smart Contract **14**

2 BLOCKCHAIN USE CASES IN INSURANCE **20**

2.1 Technology with a purpose **22**

2.1.1 Risk underwriting 24

2.1.2 Policy/Premium Management 25

2.1.3 Claims Handling 27

2.1.4 Financial Settlement 30

2.2 B3i Initiative **31**

2.3 Industry pioneers **33**

3 RISK AND CHALLENGES **36**

3.1 Cost of Adoption **37**

3.2 Security **38**

3.3 Regulation **39**

3.4 Business Strategy and Culture **43**

4 IN-DEPTH INTERVIEW **44**

4.1 Discussion and comparison analysis **45**

CONCLUSION **47**

REFERENCE LIST **48**

APPENDICES **1**

LIST OF FIGURES

Figure 1: Distributed Ledger (DL) Network 4
Figure 2: Stylized Example of a Transaction 5
Figure 3: Chain of blocks in a blockchain 7
Figure 4: Proof of Work vs Proof of Stake 9
Figure 5: Comparison between Centralized Ledger and Distributed Ledger 11
Figure 6: Public Blockchains vs Permissioned Blockchains 14
Figure 7: Smart contract model based on energy blockchain 16
Figure 8: A Smart contract-based Insurance system 19
Figure 9: How to apply blockchain in re/insurance 22
Figure 10: B3i 32
Figure 11: Architectural Overview of Codex 1 36

LIST OF TABLES

Table 1: Key differences 4

LIST OF APPENDICES

Appendix 1: Povzetek (Summary in the Slovene language) 1
Appendix 2: In-dept interviews; Methodology and Q&A. 2

LIST OF ABBREVIATIONS

AI – Artificial Intelligence

AML – Anti-money laundering

B3i – Blockchain Insurance Industry Initiative

CLS - Continuous linked settlement

DAO - Decentralised autonomous organisation

DL – Distributed ledger

DLT – Distributed ledger technology

EU – European Union

EVM – Ethereum Virtual Machine

FX – Foreign exchange

InsureTech – Insurance industry technology start-ups

IoT – Internet of Things

IOU - I owe you (an informal note that promises to pay a debt)

IP – Intellectual property

KYC – Know your customer

ONE – Open Network Enterprise

P2P – Peer-to-peer

PoS – Proof-of-stake

PoW – Proof-of-work

SaaS – Software as a Service

SEE – Sandboxed Execution Environment

SWIFT - Society for Worldwide Interbank Financial Telecommunications

TTP – Trusted third party

UK – United Kingdom

US – United States

INTRODUCTION

Blockchain has been gaining a lot of attention in the mainstream press in recent years. It has experienced significant progress during the last decade (Fuchs, 2019). Both the scientific and business worlds have shown a great deal of interest in this (Mingxiao, Xiaofeng, Zhe, Xiangwei & Qijun, 2017). Blockchain is far more than its first association with Bitcoin cryptocurrency and often these two terms are misunderstood as the same. A new sort of data structure called blockchain uses an immutable, decentralized ledger to organise transactional data (Fuchs, 2019). Aside from digital currencies and cryptocurrencies, blockchain has a wide range of possible applications (World Bank, 2017). It has the ability to completely alter the global insurance industry. Insurance is a fundamentally important institution, which makes it a great target for disturbance through technological means of risk mitigation and complexity reduction (Kim & Mehar, 2019). Insurers' possible use cases include enhancing the efficiency of fraud detection and pricing, as well as reducing administrative expenses; creating innovative products and service enhancement. Moreover, this could help with some of the key issues insurers are facing right now; pressure to cut costs and limited growth in mature markets (Lorenz et al., 2016). Blockchain and smart contracts could also help to automate regulatory reporting, improve its efficiency and transparency, enhance consistency and information quality and give regulators real-time access to signed contracts and the information from the contracts (real-time regulatory monitoring). However, the implementation of blockchain may also bring new risks to insurance companies, regulators, and customers. The intricacy of the technology, information security and privacy, the validity of smart contracts, cyber risk, integration with existing infrastructures, compatibility and standardization between various blockchains are some of the obstacles this new and emerging technology faces (EIOPA, 2021). This master's thesis aims to look into the potential use of blockchain in the insurance business, as well as to identify potential use cases and the main barriers to its adoption. This master thesis will describe blockchain by referencing literature and analyzing its current status and potential opportunities in the insurance industry. This will be achieved through in-depth interviews with insurance industry experts who are familiar with blockchain. The structure is divided into three main areas, first, one is a general introduction to blockchain its characteristics, the principles behind it and different types of distributed ledgers as well as an introduction to smart contracts. In the next chapter, we will take a closer look at how this technology could improve the insurance industry. Moreover, what are the main application areas, we talk about the B3i Initiative and its influence on the development and application of blockchain in the insurance business. Furthermore, we will take a look at the industry pioneers, who are they and what type of blockchain-based solutions they are offering in their business models. At last, we will discuss all the challenges this technology is facing, what are the main obstacles, and how they can be overcome and resolved in the future development of this technology. We will end with the research section of the master thesis, in which we want to elaborate on

the impact of blockchain on the insurance business through in-depth interviews with experts in the field.

1 BLOCKCHAIN

This chapter aims to review the important topics explored in recent blockchain literature, the technology behind it, typology and smart contracts. Firstly, we start with an introduction to the technology, its historic development, how is it defined and the main features behind it. Secondly, we talk about the consensus mechanism that has a significant impact on the functioning process of the technology. It ensures synchronization between all the nodes in the blockchain by validating the transaction before adding it to the blockchain (Mingxiao, Xiaofeng, Zhe, Xiangwei & Qijun, 2017). We explore the two most popular consensus methods: Proof of Work (PoW) and Proof of Stake (PoS). Thirdly, we talk about distributed ledger technology (DTL), how it differs from the centralised record keeping, that is currently used and what are the benefits of distributed record keeping. Also, we must present the different types of DTLs, what are the main differences, advantages and disadvantages of using permissioned or permissionless systems. In the end, we have an introduction to smart contracts, executable code that runs on the blockchain. We will explore the logic behind it, its benefits and drawbacks and briefly get familiarised with the enhancements it could bring to the insurance industry.

1.1 Introduction to blockchain

Blockchain represents one of the greatest inventions of the 21st century. Its popularity started growing in recent years, due to the knock-on effect it is having on numerous sectors. The history of blockchain starts in the early 1990s. The first form of blockchain started with a cryptographically secured chain of blocks, where it was impossible to meddle with timestamps on the documents. Later on, the system was enhanced to increase efficiency by permitting the collection of more than one document on a single block. The true significance was gained in 2008 when one person or group by the name of Satoshi Nakamoto realised a whitepaper Bitcoin: A Peer-to-Peer Electronic Cash System, the first application of digital ledger technology (Gwyneth, 2020).

First of all, let us define what is exactly blockchain and the way it operates. Takashima Ikuya in his book Blockchain: The Ultimate Guide To The World Of Blockchain, Bitcoin, Ethereum, Cryptocurrency, Smart Contracts defined blockchain as a digital, decentralized, public record of transactions of all cryptocurrency transactions. It enables participants on the blockchain to have an overview of digital currency transactions without relying on central recordkeeping since all new transactions are documented and uploaded to the adequate block in chronological order. Each node (a computer that can keep the blockchain's data, obey

protocol rules, and interact with other nodes) receives a copy of the blockchain, which is immediately downloaded. In simple terms, a blockchain is a distributed system of completed transaction records or events. Transactions in blockchain are shared among all participating parties, the consensus of the majority is applied for the verification of the transactions or events and once information enters the record it can never be erased. This indicates that every transaction completed on the blockchain has an accurate and valid transaction record. The adoption of a distributed consensus where any online activity, past or present, can be validated at any moment has the potential to transform the digital world. Distributed consensus and anonymity are two key features of blockchain (Crosby, Nachiappan, Pattanayak, Verma & Kalyanaraman, 2015). This technology is discovering applications in a broad spectrum of fields, both financial and non-financial.

In order to explain how blockchain functions, we will take a look at its components. The main content of blockchain is cryptographic hash functions, transactions, asymmetric-key cryptography, addresses, ledgers, blocks, and how blocks are chained together (Yaga, Mell, Roby & Scarfone, 2018).

Cryptographic hash functions have a versatile role in blockchain. Hashing is a technique for employing a cryptographic hash function to data that produces a somewhat unique output (known as a message digest, or digest) for inputs of almost any size (e.g., a file, text, or picture) (Yaga, Mell, Roby & Scarfone, 2018). This makes it possible for the individuals to independently check the process by taking the input data, hashing that data, and deriving the same outcome. If there is the slightest change in the input the derived output would be completely different. Some of the important properties of a cryptographic hash are the following: the function is one-way (preimage resistant) - the input cannot be derived from the output; furthermore, it is impossible to discover a different input that results in the same output. The hash function is also repeatable which means that the same data always gives the same output through a hash function; also it is collision-resistant which implies there aren't any two inputs that can hash to the same output. The hash function is unique - if there is a minimal modification in the input file the resulting hash output will be completely different (Fuchs, 2019). There are different uses of the cryptographic hash function, for example: address derivation, creating unique identifiers, securing the block data, securing the block header, etc.

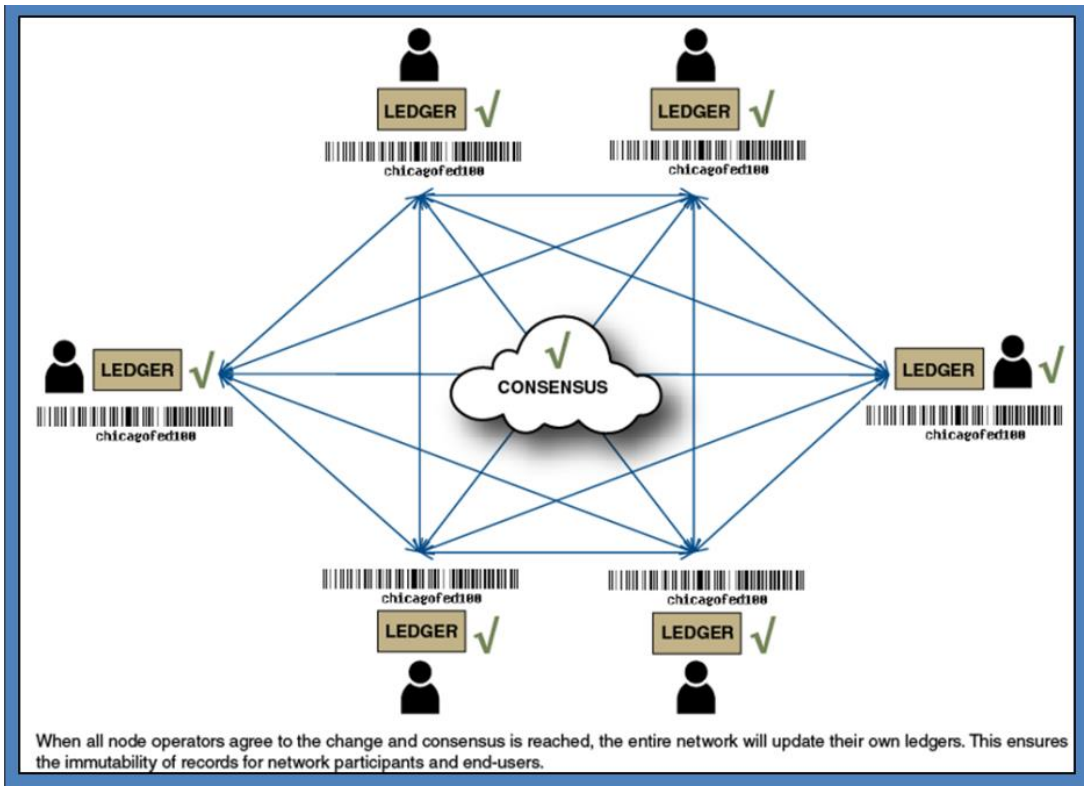
A cryptographic nonce is a random variable, a one-time code in cryptography that combined with data produces different hash digests (outputs).

$$hash\ (data + nonce) = digest \tag{1}$$

Equation (1) shows how the digest is made. You can keep the same data and use different nonce to get different digest values, this is used for the proof of work consensus model. A transaction is a process of documenting activities that occur on digital or physical assets

(Yaga, Mell, Roby & Scarfone, 2018). Figure 1 shows us the process of how transactions are created and added to the blockchain.

Figure 1: Distributed Ledger (DL) Network

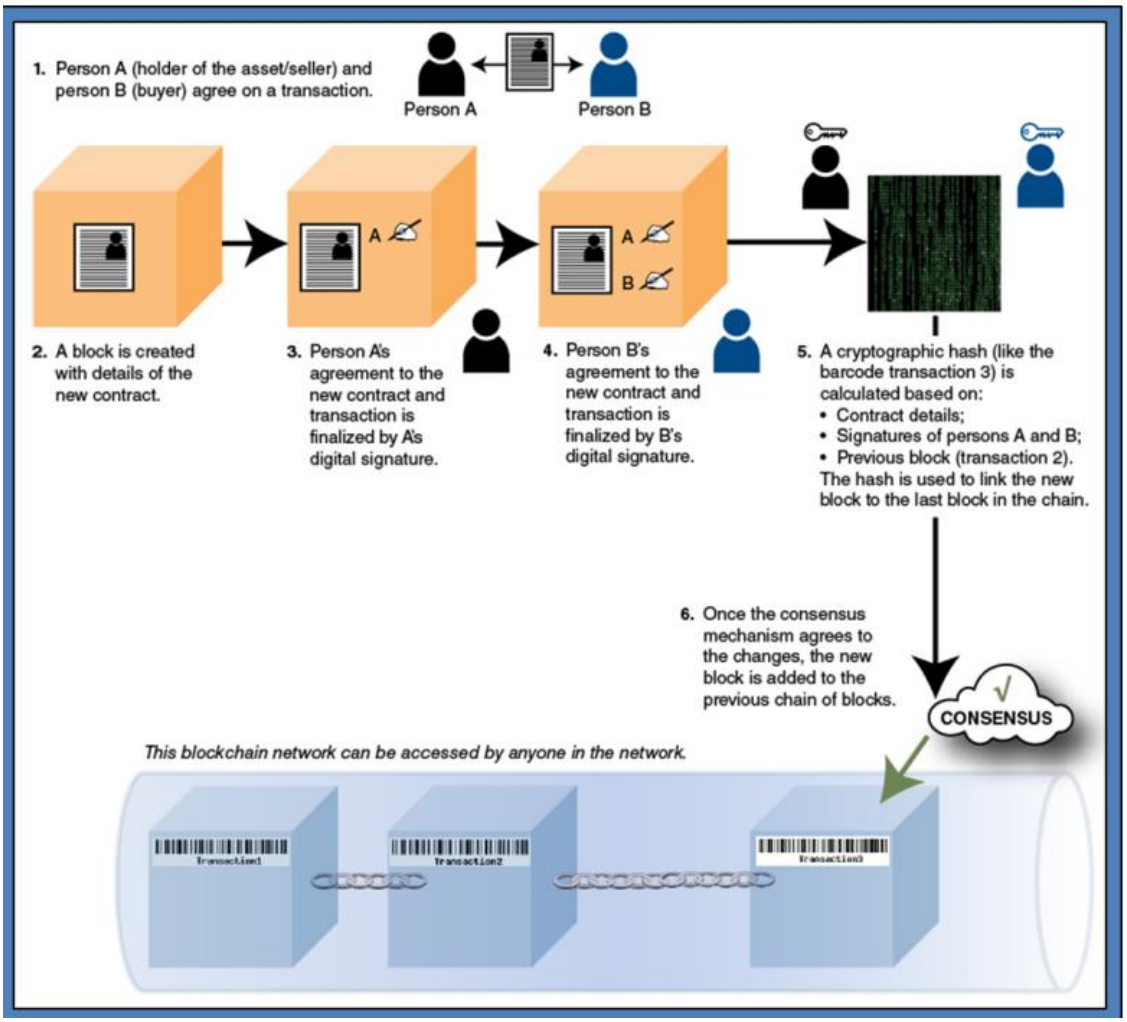


Source: Lewis, McPartland & Ranjan (2019).

A participant in a blockchain network sends information to the network in order to complete a transaction. For example, if person A wants to transfer the asset to person B, first it is necessary to determine if A is the asset's legal owner (Lewis, McPartland & Ranjan, 2019). This information is made of different data such as the sender's address (or other identifiers), the sender's public key, a digital signature, transaction inputs and transaction outputs. In most cases, inputs comprise a list of digital assets (with source reference) that need to be transferred. Regarding new digital assets, the reference is either the origin event or the most recent transaction. The sender must prove that they have access to the referenced inputs, they can do that by proving access to the private key. Outputs indicate the number of digital assets to be exchanged, the new owner(s), and a set of rules the new owners must follow to use that value (Yaga, Mell, Roby & Scarfone, 2018). After signing the transaction by both parties, the cryptographic hash is computed, which is used to tie the current transaction to the preceding transaction chain. The cryptographic hash is defined as a group of characters linked to a particular block. It is simple to validate a legal block, but it is complex to construct and insert an unauthorized transaction inside the block (Lewis, McPartland & Ranjan, 2019). A transaction can be used to transfer data, not only assets. The most important aspect of the

transaction is verifying the transaction's validity and authenticity. The transaction needs to meet certain protocol requirements, formalized data formats and smart contract-specific requirements to be validated and added to the chain (Yaga, Mell, Roby & Scarfone, 2018). The most recently created block in the chain is referred to as the chain's most recently confirmed block. After the transaction is confirmed, it is added to a block and is, therefore "chained" to the block of transactions that came before it (Lewis, McPartland & Ranjan, 2019). Transactions can be validated at any moment by the adequate public key because they have to be digitally confirmed by the sender's private key (Yaga, Mell, Roby & Scarfone, 2018). A new and updated blockchain would be emitted to all participants in the network, and everyone would have an identical copy of the master ledger (Lewis, McPartland & Ranjan, 2019). Figure 2 gives us a stylised representation of the process of adding a new transaction to the blockchain.

Figure 2: Stylized Example of a Transaction



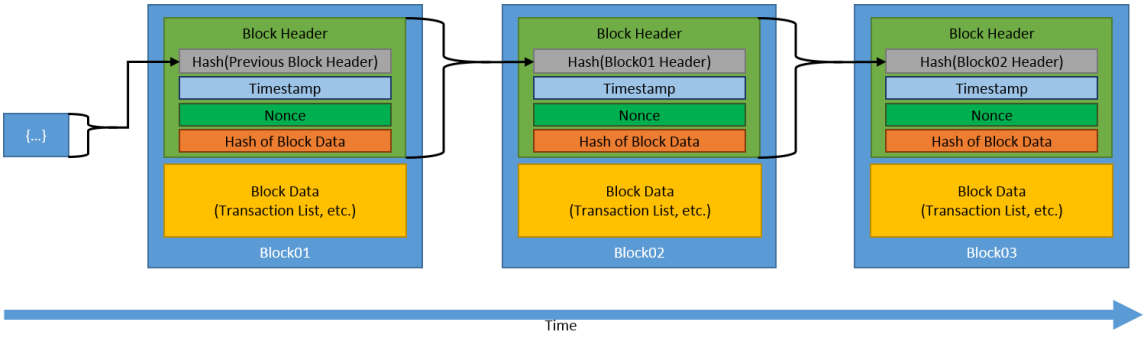
Source: Lewis, McPartland & Ranjan (2019).

Each blockchain node creates a pair of private and public keys, which are used to digitally sign transactions. The private key is connected to a digital signature mechanism, whereas the public key is connected to a verification function. For each arbitrary length input message, the private key generates a fixed-length signature string. The public key accepts the same message as input, as well as the acclaimed signature for that message. Only when the signature function generates the signature with the matching private key and the input message is the verification function legitimate (Wang et al., 2019). The task of asymmetric-key cryptography is to secure trust between users who don't know or trust each other. More specifically, by verifying the transaction's integrity and authenticity as well as keeping all the transactions public. This is done in a manner that everyone with a private key can encrypt the transaction and anyone with access to a public key can decrypt it. A single key is used to encrypt and decrypt transactions in symmetric-key cryptography.

When you apply the cryptographic hash function on the public key you get an address. Addresses serve as a public identifier in blockchain networks, they are not secret and in permissionless blockchain networks, you can create many asymmetric-key pairs, and therefore many addresses. Private keys, public keys, and related addresses can all be stored in the wallet. The security of private keys is very important because if the private key gets stolen, then any digital asset linked with that key is gone. Users must submit evidence of identification in addition to storing private keys when creating an account (Yaga, Mell, Roby & Scarfone, 2018). The blockchain-based ledger, which will allow for further advances in efficiency, is stored digitally and in a distributed manner, it has an unchangeable nature and the presence of a mutually agreed-upon consensus mechanism. Blockchain ledgers provide a different perspective on data storage, moving away from centralized data storage to a distributed one. Characteristics and types of distributed ledger technology will be discussed in detail in section 1.3.

When the transaction is validated and its authenticity has been confirmed the transaction is then added to a "block" that includes other new transactions. A block is composed of two components a block header and block data. The block header is the metadata of this block. Previous transactions submitted to the blockchain network are included in the block data. The hashing process is a process that links blocks between themselves. When the new block is full it is linked to the preceding one. Blocks that have been a part of the chain for a long time are more secure than new ones. The data is immutable which means that once a new block is uploaded to the chain, the preceding data cannot be changed. It has a chronological record of activity and the chain keeps growing when new blocks are added to the chain (Fuchs, 2019).

Figure 3: Chain of blocks in a blockchain



Source: Yaga, Mell, Roby & Scarfone (2018).

1.2 Consensus mechanisms

Consensus mechanisms play a fundamental role in the efficient and appropriate functioning of blockchain. They ensure synchronization between all the nodes in the blockchain by validating the transaction before adding it to the blockchain (Mingxiao, Xiaofeng, Zhe, Xiangwei & Qijun, 2017). The consensus mechanism's primary function is to assess if a certain transaction is legitimate or not by employing a defined specialized cryptographic validation technique designed for that DL. The consensus process is particularly significant for dealing with two key problems in blockchain applications: double spending and the Byzantine Generals Problem (World Bank, 2017). A double-spending problem occurs when a malicious node attempts to spend the same unit of currency twice or more by making additional transactions before the preceding one is confirmed (Huang et al., 2019). Although that kind of activity will be identified and stopped by an asynchronous consensus process, the efficiency of the system will be slowed because other related transactions will need to be repeated (Mingxiao, Xiaofeng, Zhe, Xiangwei & Qijun, 2017). It is essential to deal with clashes between numerous simultaneous conflicting entries, as we do not face this problem in the traditional currency because it is the entity (World Bank, 2017). In the case of Internet transactions, we have centralized trusted institutions that stop double-spending from happening. Blockchain tackles this problem through methods of verification of transactions by combining multiple distributed nodes. Byzantine Generals Problem is a problem specific to a distributed system. The data is sent through various nodes dependent on peer-to-peer connections, however, some of these nodes may be maliciously targeted, causing changes in communication content. To address this issue, nodes must identify manipulated data and ensure that all outcomes are consistent across all regular nodes. To do so we need a corresponding consensus algorithm (Mingxiao, Xiaofeng, Zhe, Xiangwei & Qijun, 2017). The two most important consensus mechanisms are Proof of Work (PoW) and Proof of Stake (PoS).

PoW is the first and most represented consensus mechanism. It is a protocol that has to be followed in order to add a new set of information entries to the ledger, as well as a new block

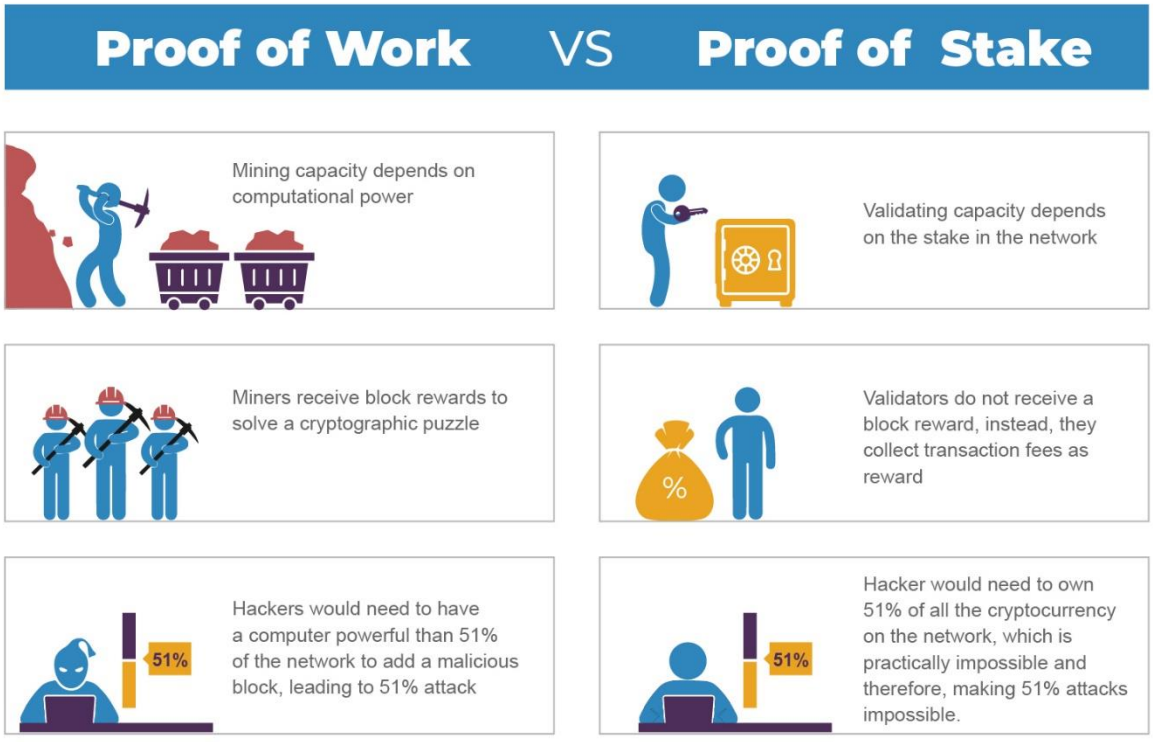
to the chain. PoW is challenging to solve regarding computing power and processing time, but it is simple to verify (World Bank, 2017). Every node in a PoW-based blockchain network must identify a nonce for its proposed new block to be able to participate in the solution-finding process that leads to consensus. The hash function output must fall within the desired range when the nonce (hashes of earlier blocks) and transactions in the new block are used as its inputs. Otherwise, the block cannot be approved (Nguyen et al., 2019). The feature of the hash function allows us to find the nonce by attempting various nonce values until we obtain an output within the desired range. After identifying the nonce, transactions and the block would be broadcasted to other nodes; the new block can be added to the current chain after being validated (Nguyen et al.,2019). Essentially, the key premise behind PoW is to hash the operation in order to compete for the opportunity to produce a new block. The winner is the first node that produces a hash value lower than the competition to reach the announced target (Cao et al., 2019). Participants compete to be the first to identify the correct node, however, the participant with the highest hash rate (computational power) may have a better chance of winning. A significant quantity of energy consumption is used in PoW consensus mechanisms. Lower-rate players typically join mining pools in order to increase their earning potential. Mining pools are collaborative pools of multiple participants, which increases their computing resources and greater chances of winning a new block than individuals. In the majority of existing blockchain networks mining pools are the dominating process of making new blocks (Nguyen et al.,2019). Since there are no shortcuts and solving "proof-of-work" puzzles is a computationally challenging task, a single node in the network has a low probability of producing the necessary proof-of-work without using a vast amount of expensive computer resources (World Bank, 2017). In the Bitcoin system, a valid proof-of-work is generated every 10 minutes, and if two are generated at the same time, the protocol with the greater difficulty score is accepted as valid ("the longest chain"). The "miner" earns Bitcoins as a reward for each valid PoW. This incentive is intended to encourage system integrity (World Bank, 2017).

Some problems may occur due to mining pools, for example, 62.7% of the Bitcoin network's total hash rate is controlled by the top five mining pools, which goes against the decentralized spirit of blockchain. Also, there is an issue of protocol delay. When a block is added to the chain, it is possible that it will not be included in the main chain due to factors such as network latency, which generates several copies of the chain, or if two participants locate two blocks at the same time. As the block goes deeper in the chain this possibility decreases. PoW mechanism is exposed to attack, in particular 51% of attacks. If a single entity has more than 51% of the overall processing power of the network, it can spend its coins more than once (in cryptocurrency networks) or obstruct other transactions by introducing conflicting blocks to the chain (Nguyen et al., 2019). This is especially a problem for small networks with limited computational power. We can conclude that the key to the security of permissionless systems is their large size. Network security is dependent on the large number

of nodes that validate accurately new changes in the ledger which enables data consistency in the network (World Bank, 2017).

To avoid the high computational complexity of PoW hash operations, PoS uses coin age. A coin's age is its worth multiplied by the period since its inception (Mingxiao, Xiaofeng, Zhe, Xiangwei & Qijun, 2017). The older the coin age the more rights the node gets in the network and the greater likelihood to win the right to add an additional block. Nodes are additionally compensated based on the age of the currency. PoS encourages the coin holders to increase the holding time because the coin age has a direct impact on winning likelihood. This may result in oligopolies or near-monopolies which contradicts the decentralized character of blockchain. The blockchain's security increases as its value rise and attackers would need to acquire a significant number of coins and retain them long enough to attack the blockchain. This makes an attack on the blockchain more difficult (Cao et al., 2019).

Figure 4: Proof of Work vs Proof of Stake



Source: Takyar (n.d.).

1.3 Distributed ledger technology

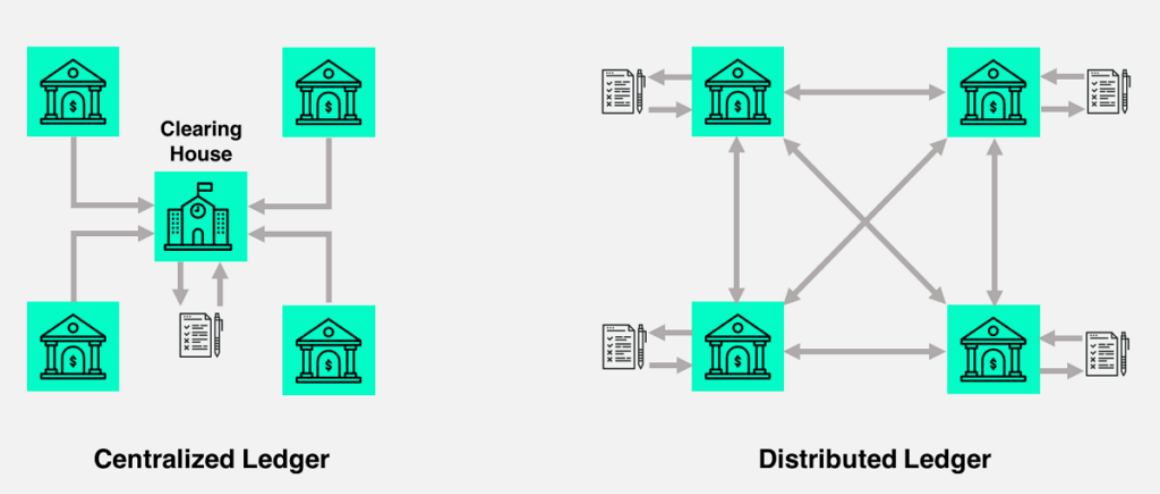
Distributed ledger technology is an innovative and rapidly growing method of storing and exchanging data across numerous data stores (ledgers). Although DLT does not have a

formal definition, it may be characterized as a collection of technical tools that enables a single, sequential, standardized, and cryptographically secure record of the transaction to be transmitted among and used by a network of community members in a secure manner. This record could include information such as transactions, asset holdings, or identity data. This is in contrast to a traditional centralised ledger system, which is owned and maintained by a single trustworthy institution. A blockchain is a type of distributed ledger technology in which records are gathered into "blocks" and connected using a cryptographic signature (Financial Conduct Authority, 2017). These ledgers have identical data records and they are also managed and governed by nodes (distributed networks of computer servers). To simplify things, we can think about DLT as a distributed database with distinctive attributes. Blockchain represents a type of DLT, it generates and verifies new data using cryptographic and algorithmic processes. This data is continuously growing, it's append-only data (new data can be added to the storage, but existing data is immutable) it takes the structure of a chain (transaction blocks) that acts as a ledger. When there is a need to add new data to the database, this process is initiated by one of the members (nodes). The new data block is encrypted and sent throughout the whole network, preventing disclosure of the specifics of the transaction. The validity of a block is assessed using a predetermined algorithmic validation technique (referred to as a "consensus mechanism") and it has to be validated by all participants collectively. Only after validation, the new block can be added to the ledgers. Every modification to the ledger is duplicated throughout the network due to this method, ensuring that everyone on the network always has access to the most recent, exact version of the ledger. Any asset that can be expressed in a digital form can use this approach for the recording of transactions (World Bank, 2017).

Essentially, we can say that DLT enables trustless parties to engage in any kind of digital data exchange on a peer-to-peer (P2P) basis with minimal or no participation from a third party. The exchanged data could be any transaction or asset that may be converted into digital form, including money transfers or storage, medical data, birth, marriage, and insurance certificates, the purchase and sale of products and services, and insurance contracts. From this perspective at least in some parts, DLT could replace the traditional intermediaries or trusted third parties (EIOPA, 2021).

We can distinguish two main DLT attributes. The first one is its capability to digitally store, record, and share "information" across all or a few participants on the network with no requirement for a centralized record keeper and no need for trust among those participants. The fact that shared information cannot be deleted increases user confidence. It is possible to conduct secure user transactions because once information has been saved, it cannot be changed without also changing all of the records. We've seen how this would benefit insurance sector by ensuring information is accurate, safe, and trustworthy (Lounds, 2020).

Figure 5: Comparison between Centralized Ledger and Distributed Ledger



Source: Shaker, Shams, & Fotohi (2021).

Historically record-keeping was centralized and there was a required trust in the data set that keeps the record or the record keeper, but DLT could remove the need for a central authority. The second attribute is to ensure that there is no "double-spending" (an event in which an individual unit of currency is used multiple times at the same time). In order not to get confused with all the different terminology because it still evolving and changing it's important to make some distinctions. Firstly, a blockchain is a technology or data type that uses encryption and algorithms to create an immutable record of data. Not all DLs are blockchains and blockchain may be applied in a variety of applications. DLs are simply shared ledgers, ledgers whose data can be shared across different participants. DLs can be permission-ed or permission-less, depending on whether a permit is needed for an entity to make a change on the ledger, additionally, they can be either public or private depending on whether anyone can view the ledgers or only network participants (World Bank, 2017).

1.4 Typologies of blockchain

The main division of distributed ledger systems is to: open ones (permission-less) and closed ones (permission-ed). Bitcoin was implemented using blockchain, as an example of a public network (Lewis, McPartland & Ranjan, 2019). In open DLs participants can read data, execute transactions or participate in the network with no restrictions, every participant may view every transaction on the blockchain, and it is accessible to any user who wants to transact (PWC, 2017). Furthermore, there is no requirement for prior approval from any entity, and members can join or quit the network at their discretion. All participants must access the network and add transactions using the appropriate software. A system with no central owner and ledger that is distributed to all network participants (World Bank, 2017). There is no need for individual databases and periodical reconciliation with their counterparties. A single database, available to everyone and an immutable record of all

previous transactions. In a public blockchain, validation depends on the cryptographic consensus mechanism, and adding new transactions to the blockchain requires large amounts of computational power to validate transactions (Lewis, McPartland & Ranjan, 2019). This high computation-based puzzle-solving makes public blockchain difficult to hack, there is a processing charge associated with each transaction (Singh & Kumar, 2021).

There have been several privacy problems identified in the context of open digital currencies. Every transaction that occurs on a permissionless network becomes a concern of public record (Gatteschi, Lamberti, Demartini, Pranteda & Santamaría, 2018). Despite the fact that users are anonymous, the specifics of payments recorded on the blockchain may, in principle, be tracked by anybody in the world with the required tools and knowledge. This means that anyone inclined to dig hard enough can find sensitive financial information stored on the blockchain. While there are methods for concealing names and the number of funds involved in transactions, they are inherently flawed and impose additional costs on users and regulatory bodies investigating financial movements as part of legal investigations (Williams, 2017). To address privacy concerns, one possible solution would be to separate the use of blockchain from the function of distributed ledger, and instead use it to transfer and document multiple transaction orders that have been encrypted for the purpose of confidentiality, but not for account balances which are used for common record of all transactions. However, to what extent this would be superior compared to currently used non-blockchain, such as those powering wire services and check-clearing systems, remains to be seen. This may paint a bit pessimistic picture of the implementations of blockchain in real systems. However, this doesn't mean that there aren't significant benefits to be gained once some challenges are addressed and resolved. Open digital currencies are the key driver of financial technology innovation (Williams, 2017).

The nature of financial services implies that a better solution would be a private and permissioned blockchain, compared to the permissionless one. Only users who fulfil the network's eligibility requirements are allowed access to private blockchains (Lewis, McPartland & Ranjan, 2019). In private DLs, members have to be pre-approved by the ledger's owner or an administrator. They regulate access to the network and determine the ledger rules. This would solve a few governmental and regulatory concerns regarding permissionless distributed ledgers, like network participant proof of identity, licensing and governance, and ownership rights of the ledger (World Bank, 2017).

On the other hand, the blockchain system's key advantage—a functioning system that functions between parties without requiring them to have any kind of mutual trust or any entity to serve as a central coordinator —is eliminated in the permissioned blockchain (World Bank, 2017). However, many essential traits and advantages of permissionless blockchains are still present in permissioned blockchains, including decentralized database storage and near-instantaneous database reconciliation. They help minimize some of the difficulties associated with permissionless systems, such as the requirement for significant computational resources to verify transactions (Lewis, McPartland & Ranjan, 2019). Instead

of relying on computationally demanding proof-of-work to validate transactions, permissioned DLs rely on various algorithmic criteria to secure member consensus. The administrator of a permissioned DL is accountable for ensuring the DL's participants are trustworthy (World Bank, 2017). The private blockchain is convenient and frequently used for individualized business solutions to keep track of data transfers among various departments (Singh & Kumar, 2021). Additionally, permissioned blockchains would be a better solution for regulatory requirements such as Know Your Customer (KYC) and Anti-Money Laundering (AML), as opposed to a private blockchain, which can restrict participants to those who have been previously vetted and are trusted, a permissionless blockchain allows for anonymous transactions that are accessible to anyone. Moreover, a private blockchain gives the possibility to control multiple tiers of access to the ledger's information. For instance, users may be permitted to view only a subset of the transaction data based on their access level, but regulators may be permitted to read all the transaction details but not add any transactions (Lewis, McPartland & Ranjan, 2019). Financial institutions do see DLs as a technological solution for maintaining client identities, processing cross-border payments, clearing and settling bond or equity deals, to self-executing smart contracts, such as credit derivatives that have automatical payout once the company fails or a bond that pays interest on a regular basis (Wild, Arnold, & Stafford, 2015). The use of blockchain may enable third parties to specialize in the analysis of data stored in the blockchain, lowering the cost of risk assessment services and assisting in the detection of money laundering or fraudulent behaviour. This would call for governance resolution of how would the blockchain access of these third parties be monitored and controlled, and how would they be accredited. Moreover, this would pose a significant concern relating to the adoption of permissioned blockchain. There would be a need for the creation of a process that determines which entities have access to sensitive information on the blockchain, and how data protection procedures are built and implemented. However, central banks as regulators of permissioned blockchains raise a question of sovereignty issues. Central banks in domestic transactions would have whatever legal authorization is needed to enable the monitoring of these transactions. On the other hand, monitoring both domestic and cross-border transactions would lead to a situation in which a central bank of one country could oversee domestic activities in another. This indicates that sensitive information about a country's economic movements would be available to foreign rivals, putting current national laws on data privacy and banking confidentiality at risk. Solving this problem would require additional layers of encryption-based security that would make sure that data is only disclosed to those with authorized excess. The main goal is to create a distributed ledger that protects unwanted surveillance of sensitive information regarding financial transactions. Restricting access does improve the security concern in the premissioned blockchain, but it doesn't eliminate it. Governance frameworks play important role in blockchain-based services, they must support the technology's long-term growth, which includes the creation of additional features that will improve privacy protections when the technology achieves a mature state (Williams, 2017).

Figure 6: Public Blockchains vs Permissioned Blockchains

	'Public' (open) Blockchains	Permissioned Blockchains
Central party	No central owner or administrator	Has some degree of external administration or control
Access	Anyone can join	Only pre-selected participants can join the network
Level of Trust	Network members are not required to trust each other	Higher degree of trust among members required (as collaboration among members could alter the ledger)
Openness	Ledger is open & transparent - shared between all network members	Different degrees of openness and transparency of the ledger are possible
Security	Security through wide distribution in a large scale network	Security through access control combined with DLT in smaller scale networks
Speed	Slower transaction processing restricts transaction volume	Faster transaction processing allows for higher transaction volume
Identity	User identity anonymous or protected by pseudonyms	Identity verification typically required by owner/administrator
Consensus	Difficult proof-of-work required as consensus mechanism	Variety of consensus mechanisms possible (typically less difficult & less costly than proof-of-work in permissionless blockchains)
Asset	Typically: native cryptocurrencies. But implementations are possible where a token is used which can represent any asset.	Any asset
Legal ownership	Legal concerns over lack of ownership as no legal entity owns or controls the ledger	Greater legal clarity over ownership as owner/administrator is typically a legal entity
Examples	Bitcoin, Ethereum	R3's Corda, Hyperledger Fabric

Source: World Bank (2017).

Both of these types of DLs have common factors, they are peer-to-peer networks, the verification method is throughout a specific consensus model and their ledger is immutable. The difference is in the approach of who can participate in the network, execute consensus and contribute to maintaining the ledger. There are different beliefs about the future scenarios for blockchain. Some predict that there will be one global public blockchain (similar to one worldwide internet) and many separate private blockchains (similar to private intranets), while others expect that a few public blockchain networks will coexist. The Internet democratises access to information (internet of information), perhaps blockchain can democratise access and storage of digital assets and become an internet of value (World Bank, 2017).

1.5 Smart Contract

A smart contract is an executable code that runs on the blockchain; in other words, when predefined criteria are fulfilled and validated, a network of computers executes the action (IBM, 2021). It is a sort of legal contract that can conduct, administer, verify, and restrict contractual performance entirely on its own (Treiblmaier & Beck, 2019). Due to the rise of blockchain in recent years and the integration of blockchain and smart contract application areas of these technologies have increased. This integration gives more flexibility to develop and design solutions for some real-world problems with lower costs and a shorter amount of

time, without the need for a traditional third-party system (Popovic et al., 2020). The earliest known definition of smart contracts and examples were introduced by Nick Szabo (1994) to better comprehend their interaction with legal and social institutions (Sheth & Subramanian, 2018). With the emergence of blockchain, this idea could be put to life. Smart contracts are traceable and irrevocable, they have value, address, functions, and state. It receives transactions as input, runs the appropriate code, and initiates the output events without the need for a third party. The smart contract became a focus area for development because of the peer-to-peer transaction and database that are administered in public in a safe and trustworthy manner (Mohanta, Jena & Panda, 2018). Due to these characteristics, smart contracts have lower transaction costs in comparison to conventional systems (Alharby & Moorsel, 2017).

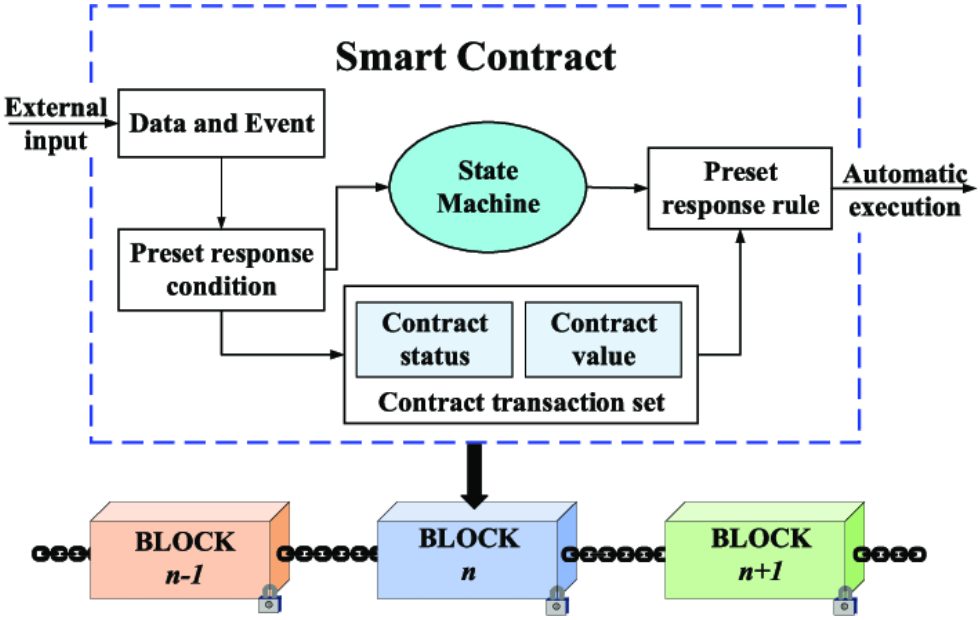
Two most important benefits of using smart contracts combined with the IoT:

1. Automation and autonomy of management activities using information supplied by affiliated devices and the need to meet the requirements for executing the smart contract.

2. "Infinite and immutable data history based on a ledger that records all data (including data provided by connected devices) ". This ensures clarity and simplicity for both the insurance company and its clients because the relevant information is accessible and protected on the blockchain with no intervention from any party (PWC, 2017, p.10).

In general smart contracts have two features; value and state. The state is recorded on the blockchain and changes each time the contract is executed. (Alharby & Moorsel, 2017). Most commonly the "If-Then" statements are used as contract clauses' triggering situations and related response actions. Firstly, smart contracts are signed and agreed upon by all participating parties, these transactions are then submitted to the blockchain network, broadcasted via the P2P network, validated by miners and placed in a particular blockchain block. When creators of smart contract store the contract they receive the feedback parameter (e.g., contract address), on the other hand, users can trigger the contract by submitting a transaction (Wang et al., 2019). A contract has a unique code that can not be changed once is deployed into a blockchain, when a transaction is sent to the contract's address the contract is run (Alharby & Moorsel, 2017). Miners in the system are motivated to use their computing resources for verification purposes due to the system's incentive mechanism. More accurately, after receiving the contact creation or invoking the transaction they execute the transaction (contract creation or execution of contract code) in their local Sandboxed Execution Environment [(SEE), e.g., EVM].

Figure 7: Smart contract model based on energy blockchain



Source: Chen & Zhang (2019).

Trustworthy data feeds know as Oracles (external inputs) and the system state decides whether the present circumstance matches the triggering requirements. If the answer is yes, then the response actions are rigorously executed, and the transaction is verified and added to a new block. A new block is added to the blockchain after the entire community has reached a consensus (Wang et al., 2019).

As we already mentioned, smart contracts may need external data (outside blockchain) in order to execute the contract. External data inputs are known as "oracles" they push data into a specific position in the blockchain at a particular time. A data feed provider for Oracle is often a third-party service built for use in distributed ledger smart contracts. Oracles gather and evaluate external data before sending it to a blockchain for use in smart contracts (EIOPA, 2021). When the smart contract receives the information from oracles they act accordingly with the new information feeds, which means either they execute or do not execute the smart contract code (PWC,2017). The key is for the parties to agree on the identity of the oracle, the source of information must be trusted and secure from hacking. Due to the blockchain's immutability, any defects or alterations of data in the oracles have no rewind or reset after the smart contract is run (EIOPA, 2021). As an example, we can use insurance for train cancellation. Oracles provide information on the arrival time of the train (from the carrier's website or a GPS sensor fitted on the train). The company Ledger proposes a hardware oracle, which uses a series of sensors to track events and solution that enables real-time information to be placed onto the blockchain (PWC,2017).

Peer-to-peer (P2P) insurance has been around for a while. P2P insurance is a risk-sharing network, essentially, people who have similar risk profiles or shared interests pool their

premiums together in order to protect themselves from a certain risk. Thus, P2P insurance enables people with similar interests to pool their risk (EIOPA, 2021). Simply said, the premise of the peer-to-peer (P2P) model is that members of a social network, often groups of up to 10 family members or friends, pool their resources to cover one another's losses and lower the cost of insurance (Abdikerimova & Feng, 2019). Blockchain has brought new opportunities to P2P insurance thanks to the decentralized autonomous organization principle (DAO). The initial stage of decentralization is smart contracts, which usually require human interaction, if a smart contract interacts with other contracts we have an "open network enterprise" (ONE). The combination of ONE and an independent agent (software that makes choices without human involvement) results in DAO, an organization that creates value without the need for a conventional management system (PWC, 2017). DAOs allow P2P insurance to increase both the scalability and decentralisation of their products and services. P2P networks could transform certain functions of the traditional insurers, new players could enter the P2P insurance market more easily which could lead to fully decentralized systems, and offer just technological services or platform providers without the main insurance company. However, this would raise a question from a supervisory aspect about the regulatory parameters and suitable regulations (EIOPA, 2021).

We can distinguish smart contracts based on whether it is influenced by the external party or not. We have deterministic and non-deterministic smart contracts. A deterministic smart contract runs without the assistance of any outside data (from sources other than the blockchain. A non-deterministic smart contract is dependent on data from an outside source (Alharby & Moorsel, 2017).

Due to its ability to eliminate the third party and automatise the system a smart contract can be used in different fields. The supply chain is one area where we could implement blockchain. A complex system of different levels of transactions, each with its own terms and conditions and multiple systems engaging at the same time. Blockchain and the DTL could make this system more transparent, trustworthy and free of third-party interference. Supply chain systems like the food processing system, transport sector, and shipment system could benefit a lot from a more reliable, open and trustful system like blockchain. “Making supply chains more transparent via smart contracts is helping to smooth out the movement of goods and restore trust in trade“ (Mohanta, Jena & Panda, 2018, p.3).

The Internet of Things and smart property; is also an area that could benefit from blockchain. Through the Internet, there are already billions of nodes that share data between themselves. If we add blockchain-based smart contracts to it, we could have nodes who exchange or acquire diverse digital properties without the requirement for a trusted third party. As an example, we have a German company (Slock. it) that uses Ethereum-based smart contracts to lease, sell, or exchange anything (for example, selling a vehicle) without using a trusted third party (Alharby & Moorsel, 2017).

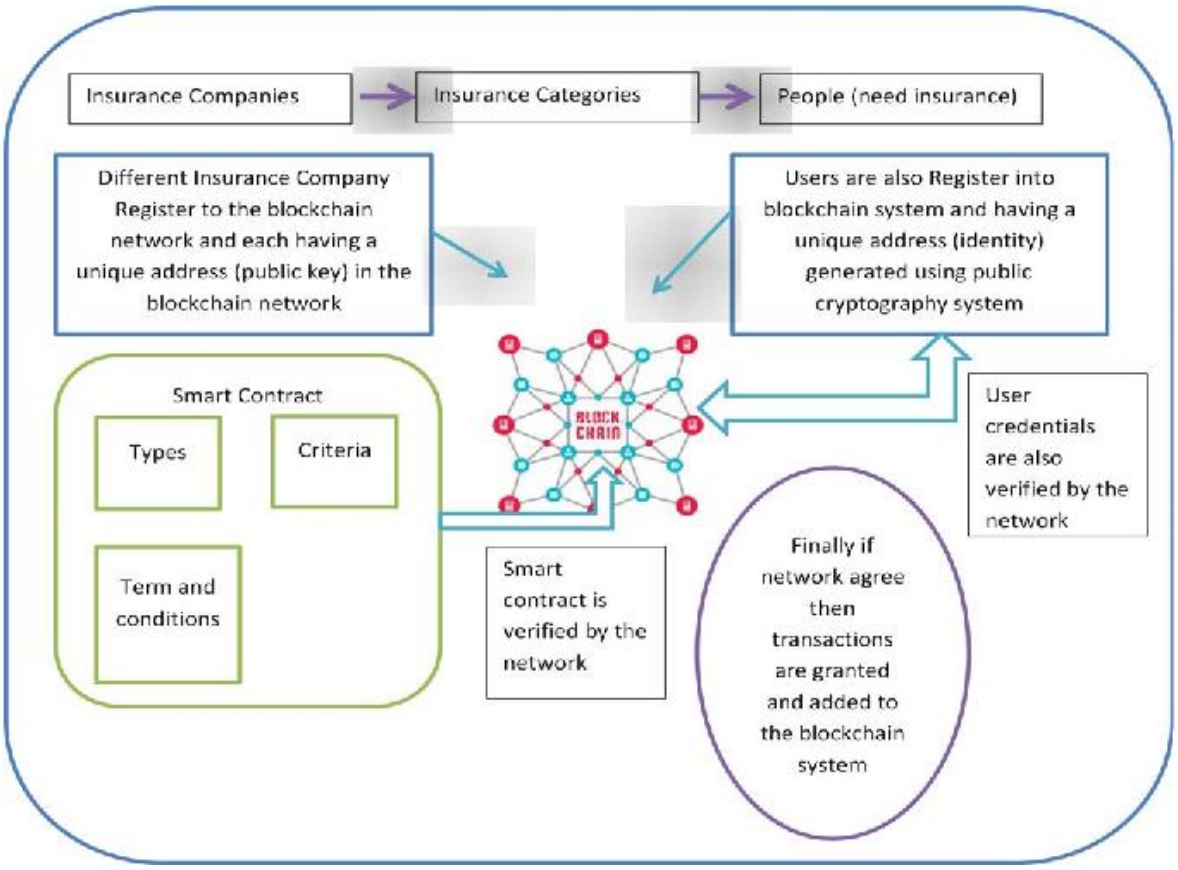
The healthcare sector may benefit from using blockchain to preserve patient privacy and store the data in a digital ledger. Blockchain may be especially helpful in situations involving patient, provider, or supplier identity verification, supply chain management, and managing dynamic patient permission to data usage (Oderkirk & Slawomirski, 2020). Healthcare systems would be more reliable and automated with the use of smart contracts. By giving detailed information on each patient's illness and any previous cases, medical records that have been converted to digital format make it easier to be retrieved and accessible to many parties in case of emergency. This would assure that the medical data whether numeric, videos (recordings) or textual images (x-rays) cannot be altered by anyone including the patient (Sayegh, 2018).

The traditional insurance system is very complex and involves different parties that participate in the process. That is why for example claim processing takes a very long time. There is a lot of ambiguity between different parties, their obligations and rights that arise from the contract. Blockchain could streamline this process making it more transparent and secure without third-party intervention. Figure 8 gives us an example of the successful execution of smart contracts in the insurance industry (Mohanta, Jena & Panda, 2018).

At last, when we talk about a financial settlement there are various methods in which blockchain can assist. The generic insurance systems require manual interactions across multiple transaction processes, causing delays in processing and prolonged payment settlement times (Raikwar et al., 2018). Blockchain combined with external systems such as SWIFT, CLS, banks etc. could be used to execute payments, a cryptocurrency made in the blockchain system, or digital IOUs/promissory notes/note payables distributed by transactors and stocked in the ledger (real money). It can also perform netting and create regular payment cycles which will optimize the settlement process. Additionally, it can also develop an internal marketplace to trade/hedge those transactions (Meeusen & Sorniotti, 2017).

Now we are going to take a brief insight into the most famous blockchain platforms that use smart contracts. These platforms offer different distinctive features in their contracts. First, we have Bitcoin, the most famous public blockchain platform that processes cryptocurrency transactions, but with relatively minimal computing power. It employs straightforward logic that demands numerous signatures to authorize a single action before ensuring that payment is permitted. The limitation comes from Bitcoins' scripting language that neither supports loops nor withdrawal limits, the only solution is to repeatedly run the code, which is inefficient. NXT is a public blockchain platform with installed smart contracts that act as templates and only allows the use of those templates which means that you can not customise your smart contract also due to limitations in the scripting language.

Figure 8: A Smart contract-based Insurance system



Source: Mohanta, Jena & Panda (2018).

Ethereum, a public blockchain platform for complex and tailored smart contracts, is the most often used platform for generating smart contracts. Because of its stack-based bytecode language and Ethereum Virtual Machine (EVM), the Ethereum platform can back withdrawal restrictions, loops, financial contracts, and gambling markets (Alharby & Moorsel, 2017).

At last, as this is still a developing technology in its early stages there are challenges and problems that this technology is facing in the real world. Contract vulnerabilities are one of those problems. One vulnerability happens when miners can control the sequence of transaction processing because many dependent transactions can execute the contract. Miners also set timestamps for the blocks they mind, they can modify the timestamps by a few seconds, this could raise a problem for smart contracts that have a timestamp as a triggering condition (money transfers). They could manipulate those contracts for their own interest. When two contracts are dependent, the contract (caller) calls another contract (callee). If the callee is abnormal, that contract is terminated and the return is false. This information may not be passed to the caller, as a result, the callee's return value must be explicitly validated to ensure that the call was correctly completed. “Re-Entrancy Vulnerability; when a contract calls another one, the current execution waits for the call to finish. As the fallback mechanism allows an attacker to re-enter the caller function, the

attacker may use the intermediate state of the caller to conduct repeated calls, leading to loops of invocations which retrieve multiple refunds and empty the balance“ (Wang et al., 2019, p.2271). The DAO attack is the most widely known reentrancy vulnerability. At the time of the DAO attack in June 2016, an attacker had stolen 3.5 million "ether" units, the money used by Ethereum, which was valued around USD 50 million. The attack was carried out by taking advantage of a serious smart contract flaw called “Recursive call”; a previously mentioned Re-Entrancy Vulnerability. As a response Ethereum community took a contentious choice to conduct a "hard fork" to recover the stolen funds. This was problematic since it goes against the ethos of blockchain's "code is law" premise. This hack raised a major security concern (World Bank, 2017).

Limitations of blockchain also represent a challenge for smart contract implementation. The irreversible character of blockchain means that once the smart contracts are distributed and finalized, they cannot be altered. Meaning that if there is an error in the contract, there is no direct way to correct it. Smart contracts' performance is further constrained by blockchains' restricted scaling, throughput bottleneck, transactional delay, and storage limits. As well as, a scarcity of reliable data feeds (Oracles) and a lack of standards and regulations. There are also two major privacy issues: 1) contract data privacy and 2) trusted data feed privacy. It is a major challenge to keep key functions and methods private, use cryptography, and prevent revealing data that should not have been publicly disclosed (Wang et al., 2019).

2 BLOCKCHAIN USE CASES IN INSURANCE

Traditional insurance is known for the long processing of claims and payments that are supervised by humans and prone to errors. Additionally, in the insurance business, there are multiple parties such as consumers, brokers, insurers and reinsurers, as well as insurance's main variable risk; all of this makes a quite complex system. Blockchain, due to its ability to provide long-term advantages like lower operational costs, increased operational automation, decreased counterparty risks, and secure and decentralized transactions can be used effectively across insurance companies (Hemanth, Fernando, Lafata & Baig, 2019). Businesses can use blockchains to achieve a competitive advantage in a variety of ways. They can improve the visibility and digitization of intellectual property ownership and payments, as well as streamline their primary business and cut transaction fees (Xu, Chen & Kou, 2019). Many researchers have considered the use of blockchain in business. In the following chapters, we will examine how could blockchain improve the efficiency of the insurance industry. First, we will discuss what are the main areas that could benefit from the implementation of blockchain in those processes. They have been grouped into four main categories; underwriting risk, policy/premium management, claims handling and financial settlement. These are all areas that are quite complex in the insurance industry, they carry high costs and risks. Improving these business processes would lead to positive change and

growth in the insurance industry. Second, we will take an insight into the B3i Initiative, a global initiative made of industry leaders and other insurance industry investors. Their goal is to address critical insurance industry needs by developing partnerships between insurance companies and other industry initiatives all over the world. The main objective is a reduction of operational risks and administrative costs which will deliver better solutions for the end consumers (Carolin, 2019). We will further examine the pilot projects this Initiative has started; how successful they are and what are the future projects and plans in the B3i community. Third, an In-depth Interview Analysis should further deepen the answers to the questions this thesis is tackling. Interviewed are industry experts who have an in-depth understanding of insurance businesses' policy implementation and decision-making abilities. They are giving their personal view on three main questions, the general impact blockchain could have on the insurance industry, discussing the possible use cases and depicting what are the main obstacles this technology is facing. We would also make a parallel between the in-depth interview of Slovene experts with the research paper "A Preliminary Study of the Impact of Blockchain on the Application Level of Insurance Industry" by Yu, Wang, Tseng & Tsao (2021) who tackle the same topic by implementing the identical research method. In the end, we will observe some of the most known industry pioneers that are trying to examine the new technology and its implementation. By using blockchain, all of the historic personal credit data, accident environmental parameters, historical policy details and all flows in the blockchain network will be stored and available in one place, if we add traditional insurance will undergo a significant upheaval as a result of the intrinsic scalability of blockchain as well as the help of the Internet of Things. Some pioneers have begun to engage in this process (Chen, Xu, Shi, Zhao & Zhao, 2018). We will take a closer look at the Ethereum platform, InsureX, the world's first blockchain-based alternative insurance marketplace, Aigang (insurance protocol on a blockchain), Lemonade (blockchain-based insurance startup) and Codex 1 (B3i's prototype).

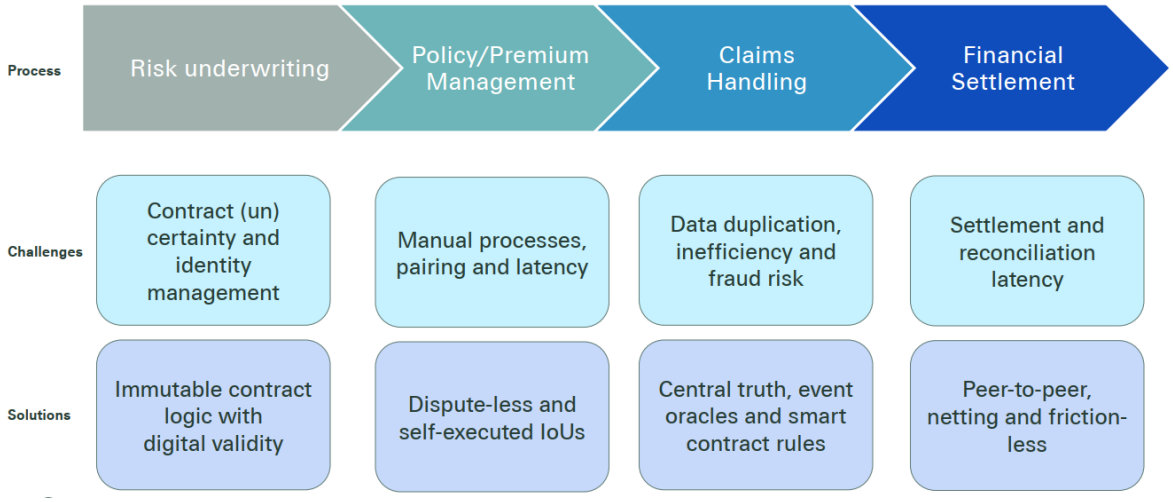
Insurance as one of the most traditional, centralized, and fortified sectors, is becoming aware of new opportunities and beginning to research new technology. Customers' growing mistrust in centralised financial institutions, which has resulted in high rates of underinsurance, is what fuels the company's modest but steadfast interest in technologies, notably blockchain. Insurance businesses, motivated by both intrigue and fear, seek to recruit blockchain engineers to assist them. Excitement arises from blockchain's promise to save time and cut transaction costs. On the other hand time, insurers are concerned that this innovation may lead to new pathways for cyber-attacks. According to the Accenture Technology Vision 2019 poll, more than 80% of insurance businesses said they had implemented or planned to implement blockchain (Bramblet, 2020). True, many blockchain insurance ventures are still in the proof-of-concept phase. To speed adoption, certain companies, such as the Blockchain Insurance Industry Initiative (B3i) or the Institutes' RiskStream Collaborative, prefer to cooperate and make coalitions.

2.1 Technology with a purpose

An insurance contract can be simply defined as an agreement where if certain particular events occur, the insurer consents to pay benefits to the insured (or a third party). Although this definition is straightforward, the administration of insurance policies can become complex. The complexity comes from, for example, claim management that needs claims adjusters to evaluate a claim and its authenticity. Another example is when parties dispute how to interpret the contract's terms, or when parties depend on representations that are outside of the policy. There is also a problem of mistrust because parties are concerned about potential fraud, abuse, or denial of claims. All of the mentioned above leads to higher costs of administration even for the simplest insurance contracts, often those costs are covered by higher premiums charged to consumers. Blockchain-based smart contracts can offer a solution for many of these problems. Many basic insurance policies have a basic "if-then" relationship that can be structured in smart contracts. In smart contracts, payments can be initiated automatically based on the objective evaluation of predefined circumstances. A blockchain-based smart contract stipulates a clearly stated policy term, and such terms can be performed by a digital protocol because the protocol can be configured to execute solely explicit policy terms. This technology could provide a solution for modern insurance problems and can structure and utilize new policy types (Cohn, West & Parker, 2017).

Swiss Re Institute has given insight into four main problems in the insurance industry that could be solved with blockchain.

Figure 9: How to apply blockchain in re/insurance



Source: Meeusen (2017).

First, we take a look at the underwriting process and possible blockchain solutions for underwriting. The underwriting process is a process of collecting information and forecasting based on different risk models and expressing the risk in currency. Underwriters

collect information from policyholders and transform it into useful data and draw relevant conclusions (Henry & Hogan, 2018). These factors represent risks to an insurance company, which can lead to liability payment in the case of some event happening as a result of these factors (Banton, 2021). The underwriting process demands a considerable investment of time and labour and blockchain could streamline these functions. Blockchain would enable more accurate data that would enable both parties, insurers and policyholders to quantify and mitigate risk more efficiently. The main idea is to collect information through affiliated devices, systematize it on a blockchain and apply artificial intelligence to evaluate the data, which leads to more accurate premium determination. This will reduce the cost of underwriting and help with the process automatization and reduction of time in processing the underwriting policies (PWC, 2017). It is the ideal tool for auditing/resolving disputes since terms and obligations are encoded in a computer program with no room for ambiguity and the state is irrevocably preserved in the ledger. Due to the possibility of DL being private, all the terms can be kept secret from all but the legitimate parties. In the private DL strong identity management is in place and because of that, it is easy to identify participants. It is unnecessary to use a centralized identity system since each organization in a permissioned blockchain has the exclusivity to issue credentials for its entities, and the entity's membership to the organization must be validated by everybody else in the blockchain (Meeusen & Sorniotti, 2017).

Once we define who is who, and who can do what and we express the business logic in chain code, the contract activation and realization are quite simple. This system helps with the policy/management system because of the immutable ledger and predefined rules that help avoid/settle any disputes. Moreover, blockchain could improve and simplify some of the time-consuming and costly procedures, such as KYC/AML procedures (Grima, Spiteri, & Romānova, 2020). There is also potential for reduction of identity theft and other cyber liability losses since it can authenticate the validity, ownership, and supply of commodities, as well as the legitimacy of papers.

When we talk about claim management there is also a useful application of blockchain. As we already know, the ledger is a globally recognized and verified source of truth for all users, recording all transactions that occur in the system. In claim management, we also have an exogenous variable, for example, the event in the real world that triggers the claim or currency conversion. How can blockchain learn about the facts in the real world? Blockchain systems use so-called oracles that can be either trusted third parties operating as sources of data or a majority's aggregate input.

In the end, when we talk about a financial settlement a blockchain can assist in a variety of ways. It could be the use of a payment interface with external entities (SWIFT, CLS, banks), a cryptocurrency embedded within the blockchain system, or digital IOUs/promissory notes/note payables produced by transactors and kept in the ledger (real money). It can also perform netting and create regular payment cycles which will optimize the settlement

process. Also, it can generate an internal marketplace to trade/hedge those transactions. (Meeusen & Sorniotti, 2017).

2.1.1 Risk underwriting

The underwriting process is a process of evaluation and risk analysis that comes from insuring people and assets. It is a process of pricing risk that comes from an insurance contract. Essentially, the underwriting process is a process of collecting information and forecasting based on different risk models and expressing the risk in currency. After collecting the information from policyholders, they need to transform the information into useful data and draw relevant conclusions from it (Henry & Hogan, 2018). In order to determine the probability and the impact of a risk underwriters use specific software and actuarial data. The essential role of the underwriter is risk assessment prior to the policy period and at the time of renewal. In the underwriting process, it is very important to take into consideration all the factors that can influence the insurance contract. These factors represent risks to an insurance company, which can lead to liability payment in the case of some event happening as a result of these factors. Based on the platform's assessment and the integration of all data given by the underwriter's observations, the system creates a suitable premium (Banton, 2021). This requires a considerable time investment and labour, blockchain optimizes these processes. Its use can be beneficial for both parties, insurers and policyholders because it would enable more accurate data that would enable both parties to quantify and mitigate risk more effectively (Henry & Hogan, 2018). By using blockchain in the underwriting process, external data can be included which will reduce the liability risk and administer semi-automatic pricing (Derebail, 2018). The accuracy and effectiveness of the underwriting process can be improved by insurers utilizing the blockchain-based ledger and smart contract features, as well as the IoT data collection capabilities and artificial intelligence's potential to process data. The basic goal is to gather data from connected devices, organize it on a blockchain, and analyse it using artificial intelligence so that premium calculations are more precise. This will lower the cost of underwriting, aid in the automation of the process, and speed up the underwriting policies' processing time (Aggour, Bonissone, Cheetham, & Messmer, 2006). Furthermore, there has been some recent research in pricing that has shown how dynamic and static behavioural variables affect risk. These movements are quite important for insurers to capture. In the blockchain environment, these behavioural changes could be gathered and exchanged on a blockchain, that would almost instantly adjust and optimise the real-time pricing on real-world data recorded on the blockchain. This is still just an idea in the making, there is a lot of analysis and research to be done. The insurance sector will transform; into a world where voluntary data interchange and the ability to continually evaluate individuals' behaviour and risk profiles would result in dynamic pricing and dynamic, customizable, and personalized insurance products, as well as risk mitigation (PWC, 2017).

Blockchain would improve transparency and trust by allowing shared visibility in large-scale global projects. The first global insurance policy to use blockchain and smart contracts to provide insight into underwriting coverage and premiums at the regional and global level were successfully implemented by AIG, Standard Chartered, and IBM last year (Derebail, 2018). The insurers will concentrate on innovative data-collection strategies because there are already some initiatives by insurers that offer a reduced premium for exchanging real-time driving data, whether through aftermarket monitoring or by distributing manufacturer driving data (Henry & Hogan, 2018).

A high level of capital requirements and capital regulation is one of the insurance industry's characteristics. They are needed due to the business nature and need for consumer protection. There are high entry barriers, underwriting guidelines are defined individually by each company and the market is dominated by a few major players. The structure of incentives in the blockchain design has the potential to reduce the need for capital requirements and capital regulation. In the traditional centralized structure, the insurance firm is looked at as a single entity and the capital requirements are calculated based on the standard deviation of total payouts. The main idea of reducing the capital requirements – i.e., reserves needed to meet the unexpected component of payouts in the blockchain structure is based on assumption that a good system is in place to secure an adequate amount of tokens for each underwritten policy, and every agent is responsible for meeting the payouts of the underwriting policy. Moreover, this means that the capital adequacy falls on the individual agents, agents will determine the amount of capital needed based on how much additional risk the potential underwriting liabilities contribute to the agent’s overall portfolio. Therefore, it is possible if the incremental risk to the private portfolios of the agents from the contingent liabilities is small enough, that the sum of the individual amounts held by each agent would be less than the capital requirements held by a traditional corporate entity (Calcaterra, Wulf & Rao, 2019).

2.1.2 Policy/Premium Management

All of the involved parties in the insurance process (brokers, insurers and reinsurers) must conduct KYC/AML checks on each of their counterparties. The KYC/AML also depends on the regulators, a single transaction can involve many participants, from brokers to underwriters to reinsurers and all of them have to do KYC/AML. These repeated checks represent additional costs and delays for each participant (Mainelli & Manson, 2016). This costly, time-consuming process of compiling client and stakeholder documentation ("Know Your Customer", or KYC) could be transformed by distributed ledger technology (PwC, 2017).

One of the most significant features of blockchain is the high level of confidence it fosters. It has the potential to eliminate fraud due to the capacity of validating the legitimacy, ownership, and supply of commodities, as well as document authenticity. Blockchain can be

connected with external databases, which means it can be connected with police reports that would quickly detect the behavioural patterns associated with a particular identity. Additionally, it would demonstrate the day and time a policy was issued or a product was purchased, as well as any future ownership and location changes. By offering a decentralized digital repository blockchain has the ability to remove errors and identify fraud it can objectively check the authenticity of clients' claims and policies as well as give a detailed transaction history. This eliminates transactional repetition and the need for a centralised entity and creates a public record of all transactions. Furthermore, blockchain may contain encrypted personal data as well as a public ledger. Some companies are already utilizing it to reduce fraud and liability connected with cross-border and multi-currency payments (Chekriy & Mukhin, 2018).

However, the current data centralized model puts organizations at risk. Every organization compiles a variety of paperwork for a certain consumer, but none of this information is shared (Chekriy & Mukhin, 2018). Moreover, an estimation is that 5 to 10 per cent of all claims are fraudulent. US non-health insurers lose more than USD 40 billion per year due to fraudulent claims, according to the FBI (Lorenz et al., 2016). The amount of cyber-attacks is increasing, as well as thefts of millions of consumers' personal information (Chekriy & Mukhin, 2018).

Information is secure on the blockchain because data is not kept in a centralized database. By pooling operations through a shared, encrypted database, blockchain would yield significant benefits (PwC, 2017). There is also potential for the reduction of identity theft and other cyber-related risks. The data is encrypted at the financial transaction level, which means that identifying information on the blockchain is quite limited and that minimises the risk of identity theft. Cyber liability is the risk that a third party possessing an individual's data may disclose personally identifiable data (Chekriy & Mukhin, 2018). Currently, this data is stored at a central location and has software that protects it from hacking. The blockchain data would be executed and saved using the existing blockchain without decrypting the underlying data because the chain can be independently validated by separate nodes (Chekriy & Mukhin, 2018).

PWC in cooperation with Z/Yen has developed a model to perform outsourced customer identification verification. Several legal concerns around data security and privacy are resolved by using blockchain to store all of a client's papers and proof of validity. All documents are encrypted, only the consumer has the keys. The consumer would be able to share the keys with institutions with whom they want to do business and the institutions could rely on that information as valid. This would reduce the cost and time delays of KYC/AML processes in the industry (Mainelli & Manson, 2016). Furthermore, according to Goldman Sachs, continuous and integrated application of blockchain in the banking industry might save the industry roughly US$ 3 billion to US$ 5 billion in KYC and anti-money laundering (AML) expenditures every year (PwC, 2017). This technology could be very helpful also when applied in a smaller range, for example between groups and their

subsidiaries in cost reduction. All existing valid data is already stored on the blockchain so there is no need for cadre to focus on KYC tasks, which, reduces processing time and enhances client experience. Errors in the claim payments would be reduced because the decentralized and immutable system would be less likely to allow false billings and tampered documents. This technology would help insurers to reduce their loss adjustment costs and consequently offer consumers lower rates (Chekriy & Mukhin, 2018). Blockchain can lower operational and administrative expenses by automating verification of policyholder identity and contract legitimacy, claim registration, third–party information and claim payouts in an auditable manner using a blockchain-based payment framework or smart contracts. Customers will enjoy better service and pay reduced premiums as a result of controlled access to claims and claims histories on the blockchain, which also improves administrative operations (PwC, 2017). In order to achieve the full benefit of blockchain application in this process, it is necessary to intensify collaboration between insurers, manufacturers, customers, and other parties exciding the current standard database systems and collaboration forms (Lorenz et al., 2016).

In the insurance business, customers have a small possibility of knowing how their data is handled. More specifically, if their data is shared with third parties, thus they face extended claim processing time or claim refusal while the premiums are getting more and more expensive. This leads to a lack of faith in insurance companies. On the other hand, if numerous insurance companies would choose to distribute data in the decentralized and shared ledger this could give them some considerable advantages. It could lead to the better building of customer profiles and eliminate the duplicity of the records, this data would be trustful because of ledger immutability. Customers would also gain more trust in insurance companies because they will have an insight into how their data is shared and processed. Adding also the possibility of a claim automatization process using blockchain which can accelerate the claim payouts. In the end, in blockchain, an insurance firm can track all of those chained transactions and automatically validate third-party claims or payments (Kot, 2020).

2.1.3 Claims Handling

Claim handling is a complex process that involves a series of processes that each handler goes through when a new claim is submitted. It involves collecting information, analysing, planning, and implementing a settlement strategy. This process could be repeated several times over the life of a claim, depending on the intricacy of the specific situation and the accessibility of information. In order to have an efficient and qualitative claims-handling process, it is essential to have the right information, which depends largely on the first step, information gathering (Koscielecki, 2018).

Companies that hold on to the traditional approaches; of slow and heavy paperwork will lose to their competitors that are more digitally savvy because the automatization of claim

management enables them to offer lower premiums to consumers (Kot, 2020). Making a claim is usually a long and confusing process for a policyholder. They have to face a long and exhausting process of consolidation between the insurers and reinsurers. This process includes different types of contracts, which ones are accurate, who has already made a payment, and which ledger contains the proper accounting. It's a process that is complex by its nature, even when we are not taking into consideration the extra time to follow up on the regulations for combating fraudulent claims (Derebail, 2018).

In the case of claim notification, there can be a lack of information which means that the most appropriate strategy cannot be developed, or there is some additional information that changes the strategy once it is disclosed. This can lead to the claims handlers' need to collect and verify the relevant information from numerous sources, such as members, surveyors, brokers, municipal governments etc. This information is then distributed to other relevant parties such as external legal teams (sometimes in several jurisdictions), brokers, and correspondents. A significant amount of time is devoted to promptly distributing information and keeping everybody informed about changes that happened. All of these characteristics contribute to the process being sluggish, inefficient, complicated, and frequently costly. The longer it takes to resolve a claim, the longer insurers must keep their reserves at the same level (Koscielecki, 2018).

The use of blockchain could make this process much more efficient and effective. Our information would be available on a distributed ledger that is accessible to all relevant parties simultaneously, including claim handlers. Policyholders can easily file a claim on the blockchain, and upon reporting the claim, all essential information would be acquired immediately from the appropriate sources. All policy details would be instantly sent to all relevant parties simultaneously. This would allow insurance companies or claim managers to begin formulating the best resolution approach right away, saving them the time it would take to email policyholders and other stakeholders for more information. The relevant information is available, and claim executives can, if necessary, use additional resources, such as qualified specialists or outside legal teams (Koscielecki, 2018).

True modernization of insurance administration entails a rise in customer and insurer confidence. For this to occur, there must be a significant number of well-known participants in the blockchain ecosystem. As an example, the Bank of China has collaborated with top insurance companies and developed its blockchain. After new records are submitted to the blockchain, distributed ledger technology facilitates updating and validating the data against other entries in the network, which substantially lowers operational costs while also ensuring high transaction security (Kot, 2020).

The loss notification process could be substantially improved by streamlining it in the blockchain. The technology would enable full straight-through processing for simple claims with predictable characteristics and patterns, claims would be resolved more quickly and all the parties' claim handlers would ensure coordination and provide more rapid payouts to

service suppliers if they could instantly verify the status of claims (Cultu, Ganjani, Larrea, & Müssig, 2022). Claims that need additional investigation are identified much faster. Another vital improvement would be in the management of claim data quality and volume, which could be important for recognizing claim patterns for risk control teams to manage. The relevance of blockchain applications in claim handling has been acknowledged by many industry leaders and other connected parties such as large business consultancies etc. Claim handlers have already shown an interest to understand the perks of blockchain in the claim-handling process because of the transformation this technology will bring to claim handling in the future (Koscielecki, 2018).

There is also one more important factor to mention that we will discuss further on in the next section, the need for bank transfers. Bank transfers additionally slow down the claim handling process, usually, it takes weeks for the customers to receive their payouts. This will be the case until the banks and insurers get to an agreement and the payments could be completed without significant delays if they create a single mechanism they can rely on (Kot, 2020).

The adoption of blockchain for policyholders would imply claim automation and data commodification. They should be aware of the negative consequences that automation and commodification may have, but they should also take advantage of any potential cost-saving advantages, particularly premium reduction (Kumar, 2020). Automatization of claim handling could considerably benefit the policyholder. For starters, reducing payment time increases liquidity and cash flow, permitting companies to execute recovery operations more effectively once the covered event occurs. Reduced administrative and overhead expenses for first- and third-party claims will benefit both policyholders and insurers. However, policyholders should take precautions when committing to blockchain-based claims-automation programs since claims automation without appropriate policyholder controls might deprive policyholders of essential input. The typical claim reporting procedure requires the policyholder to choose the optimal approach for managing and reporting the claim in order to achieve maximum possible coverage while correctly portraying the triggering event. For ordinary claims, this procedure might be straightforward and mechanical, but it can also be sophisticated and customized for unique or important claims. Because of the nature of the automated information-reporting system, this might result in the rejection of potentially covered claims in the case of complex claims. Policyholders need to be very aware of what parts of a claims management process are automated, what information is provided, how that information is presented, and if the policyholder may use a method to challenge automated claims judgments. Automation of claims compromises the trade-off between maintaining pre-paid insurance coverage and corporate efficiency. Essentially, lowering the cost of complicated international insurance programs using blockchain is economically profitable to the policyholder, irrespectively of whether the policyholder keeps the risk or transfers it to an insurer (Henry & Hogan, 2018).

In conclusion, blockchain can help insurance businesses obtain, organize, and analyze data more effectively. The blockchain's ability to communicate data in real time makes premium calculations more precise and efficient. More effective measurement and risk mitigation would be beneficial for insurers and policyholders (Chen, Deng, Tsaur, Li, Lee, Wu, 2021). However, policyholders should be careful about the sort of data supplied to insurers, its structure, and the time of access to that data in order to avoid losing proprietary data in return for lower rates. Policyholders need to control access to their data because unrestricted data access could lead to reduced or completely eliminate of the value of proprietary data. It is critical to assess the short-term benefits of reduced premiums against the long-term costs of handing up significant proprietary data to insurance firms. Data protection and cost-saving balance are highly important to keep. Handled in the right way blockchain should be beneficial for both policyholders and insurance companies, handled badly it can lead to the loss of valuable proprietary data for policyholders. It is important to be very cautious while implementing this new technology in order to keep the benefits for both insurers and policyholders (Henry & Hogan, 2018).

2.1.4 Financial Settlement

Financial institutions, such as banks and insurance companies should consider their needs when deciding whether and how to use digital money and blockchain. More specifically, how could they benefit from using blockchain for financial settlements in the insurance industry (Williams, 2017). Settlements have been perceived as labour-intensive, time-consuming, and vulnerable to tampering and monopoly power, blockchain would remove these issues. They would no longer take days, lemons and fraud can be avoided, and these consequences will very certainly have an impact on the agents' ex-ante incentives in the economy (Cong & He, 2019).

Efficiency improvements are among the biggest advantage of employing blockchain in the settlement process. Moving settlements to decentralized technology improve the settlement process by reducing transaction costs and hazards. On the other hand, the main settlement risk is the counterparty risk, the risk of default on obligations which shouldn’t be underestimated since it can lead to substantial financial losses. Therefore, in centralised systems, this risk is mitigated through financial intermediaries (Sandner, 2020). In peer-to-peer blockchain systems, transactions would immediately transfer money from one participant to another. This might be carried out via a deferred net settlement or a real-time gross settlement in which numerous transactions' balances are shifted simultaneously. While real-time gross settlement provides an important benefit to financial service clients, delaying net settlement would help shield sensitive information from mass exposure (Williams, 2017). But we also need to talk about the operational hazards. The blockchain systems' associated software has to be operational round-the-clock. This means that any problems that may occur with the software, such as power outages, internet outages or hardware problems can lead to temporarily unavailable service (Sandner, 2020). These relatively minor concerns should not

take advantage of what this technology is offering, the potential to accelerate the money transfer procedure, so that international money transactions could be completed in minutes rather than days (Williams, 2017). Furthermore, there are also software-related risks, such as bugs in smart contracts. These risks should not be overlooked because of the complexity of smart contracts and their interconnection which could lead to a serious risk increase in the insurance business. A blockchain-based financial settlement might be utilized for immovable property, products, or services that are purchased for money or traded for other assets, in addition to financial assets. This essentially means that all consumption and trade procedures are covered, and the expenses associated with these transactions may be greatly reduced. Companies should now evaluate the benefits of tokenizing physical assets and adopting DLT for their industrial use cases as regulatory handling of digital assets becomes more transparent. Furthermore, in order to allow effective blockchain-based settlement, the euro must be tokenized as a type of commercial bank money, e-money, or central bank money (Sandner, 2020).

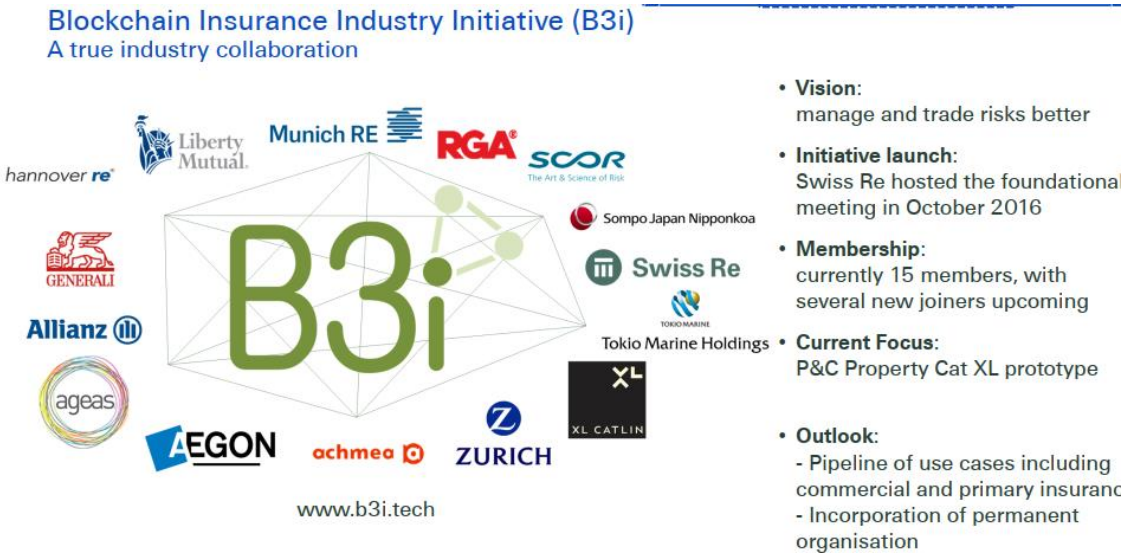
2.2 B3i Initiative

Insurance companies are taking seriously these new possibilities with blockchain, According to the 2019 Accenture Technology Vision study, more than 80% of insurance businesses either now use or plan to use blockchain. Even though the majority of these blockchain insurance initiatives are still in the proof-of-concept stage, some businesses have opted to join and build alliances in order to accelerate the process, such as the Blockchain Insurance Industry Initiative (B3i) (Consensys, 2021). B3i is a global initiative created by industry leaders and other insurance industry investors. It was created in 2018 and currently, there are more than 40 companies in the B3i. Their goal is to address critical insurance industry needs by developing partnerships between insurance companies and other industry initiatives all over the world. The main objective is a reduction of operational risks and administrative costs which will deliver better solutions for the end consumers (Carolin, 2019).

The B3i mission is to use blockchain to develop industry standards, protocols, and network infrastructure that will remove friction in the value chain and risk transfer processes. So far, value chains in the insurance industry have a high degree of manual processing and reconciliation, with multiple parties participating and using different types of shared information. This leads to high costs, slow turnarounds, and frequent errors (R3, 2020). B3i believes that by acting together, the insurance industry can improve the efficiency of transactions, reduce operational risk, reduce foreign exchange risks, and improve the quality and robustness of data. They see blockchain as infrastructure distributed between its members and their partners to conduct B3i-developed standardized business processes that are carried out by smart contracts. B3i members are primarily reinsurers, but also insurers are members. It was created to investigate the possibility of adopting [blockchain] inside the industry in the interests of all stakeholders along the value chain (Kim & Mehar, 2019). Additionally, streamlining the reinsurance settlement process speeds up overnight cross-

border payments and decreases the time it takes to calculate quarterly payments for businesses with multiple contracts, improving financial reporting for insurance firms. B3i debuted a prototype blockchain reinsurance policy, with a non-member testing phase beginning in 2017. Furthermore, this prototype supports multilateral payments, smart contracts, functionality (including layered logic), and on-chain processes for approvals, settlements, and asset exchanges (Henry & Hogan, 2018).

Figure 10: B3i



Source: Meeusen (2017).

According to Willis Re, the consortium has focused on the development of contracts between reinsurers for the automated calculation of catastrophe reinsurance claims and the evaluation of the reinsurance post-placement processes (Kim & Mehar, 2019). The smart contract management system is intended to optimize risk trading by automating some of the catastrophic reinsurance activities that are now handled by brokers. Blockchain can reduce the requirement for participating companies to balance their reinsurance accounts on a regular basis by providing transparency across the entire value chain (IBM, 2018). The prototype would be granting access to the same distributed ledger that is cryptographically secured that would bring together insurers, reinsurers, and brokers on a single platform. The cedent company would be able to fill in precise information about the contract parties, interaction would stay on the platform until a settlement is achieved. Encrypted information would be accessible to each party, but only relevant information would be visible. For example, if you are a broker and your commission is contingent upon the policy being bound or a specific portion of the contract being executed, having visibility and transparency to ensure you see that trigger when that event actually occurs prevents the cycles of phone calls and follow-ups that typically occur (Writer, 2017). On the same platform, each reinsurance contract is created as a smart contract containing executable code. This implies that if a claim

(earthquake, hurricane, etc.) occurs, the smart contract will examine the relevant data on the platform and make appropriate compensation to all impacted parties (Sayegh, 2018). Additionally, the primary insurer of catastrophic insurance hedges its own risk by reinsuring with a syndicate of reinsurers. Blockchain's mission is to streamline those business processes that take place after syndicate partners' terms and conditions have been determined, such as processes for passing on updates across the syndicate (Kim & Mehar, 2019).

Allianz in cooperation with startup Adjoint is working on a solution to reduce foreign exchange risk. The project is in the advanced stage of testing an internal token to move around its global affiliates without having to deal with currency conversions. According to an Allianz representative, the company is still investigating blockchain's potential to automate and accelerate international insurance payments for its business clients. A research team is working on creating a token-based digital payment system that will enable smooth, straightforward, and fast money transfers for a variety of different forms of payment (Kim & Mehar, 2019). Allianz Re Blockchain expert said that one of the goals of the B3i project, which they have seen in numerous use cases for reinsurance products, is to create contractual governance between reinsurers and primary insurers in order to modernize the supply chain from the policyholder to the principal insurer to the reinsurer to the retrocessionaire, ultimately reaching the capital market. The initiative intends to employ artificial intelligence combined with blockchain to automate such procedures without compromising the entire system, therefore it's like turning a manual system into an automatic system enhancing operational efficiencies and pushing technology toward the next level. That is what B3i is looking at on a global scale (Sayegh, 2018).

2.3 Industry pioneers

Because of the complexity of traditional insurance policies that require human supervision and include consumers, brokers, insurers and reinsurers the system is prone to errors. Due to the swift growth of new technologies like big data and artificial intelligence, the traditional insurance sector experienced significant changes in recent years. InsurTech has emerged, referring to the use of innovative technologies, such as big data, blockchain, and artificial intelligence in development, pricing, marketing, and claims processes. InsurTech is crucial for enhancing the insurance ecosystem and addressing industry-wide problems (Cao, Lyu, & Xu, 2020). Industry leaders worldwide have seen an opportunity in blockchain application in their line of business. The market's quick organization of B3i-type projects is a great sign industry has acknowledged the potential value of blockchain and the barrier has been crossed (PWC, 2017). This change in the market is mostly driven by the insurance industry leaders, but every company needs to create a unique approach depending on its priorities. Results so far seem very promising, but volumes are still low. Blockchain application would be a considerable driving force that will change the productivity implications for all the players in the system. Besides the pilot projects from the industry leaders, there is also a task group that focuses on collaboration with associations and regulatory bodies and strives to find

solutions for problems that restrain blockchain from becoming a leading technology in the insurance industry (PWC, 2017). We will observe some of the most known industry pioneers that are trying to examine the new technology and its implementation. Through the use of blockchain, all historical data, including individual historic creditworthiness, accidental environmental parameters, historic public data, and all activities in the blockchain network, will be kept and available in one location. Traditional risk-selling insurance will experience a tremendous change when paired with the intrinsic scalability of blockchain and the cooperation with IoT. Some forerunners have begun to participate in this process (Chen, Xu, Shi, Zhao & Zhao, 2018).

Ethereum is one of the most known open-source, public blockchain-based distributed systems that enable developers to create and distribute software applications, and it is powered by its cryptocurrency token, ether (Dattani & Sheth, 2019). As a permissionless network, any node may join by creating an account on the Ethereum platform; it employs the EthHash PoW consensus model (Singh & Kumar, 2021). It is also known as the most common platform for developing smart contracts. On the Ethereum platform, you can reliably deliver and execute smart contracts. With the aid of a Turing-complete programming language, the Ethereum platform can handle complex and customizable smart contracts; withdrawal limitations, loops, financial contracts, and gaming markets are all supported by the platform (Alharby & Moorsel, 2017). Ethereum Virtual Machines are miner nodes, miner nodes provide cryptographic tamper-proof tenacious execution, and the Ethereum Virtual Machine executes stack-based bytecode used to create smart contracts (Singh & Kumar, 2021). Various high-level languages can be used to build smart contracts (for example, Solidity, Serpent, and LLL), and the codes of those languages may be combined into EVM bytecodes and run (Alharby & Moorsel, 2017). Ethereum can be regulated and configured through various IoT devices, it is compatible to interact with other blockchains and besides smart contracts, it is capable of running other decentralized systems (Singh & Kumar, 2021).

As a product of the collaboration between insurance giants from the Blockchain Insurance Industry Initiative (B3i), we have InsureX, which aspires to tackle the shortcomings of the current insurance system by being the first blockchain-based alternative insurance marketplace in the world (Chen, Xu, Shi, Zhao & Zhao, 2018). InsureX platform operates on the Ethereum blockchain, a Software as a Service (SaaS) platform. It offers a more streamlined experience, access to a broader array of products and lower commissions for both organizations and individuals. The platform is entirely electronic and secure, allowing safe transfers of confidential documents such as medical records or financial information (Crunchbase, 2017).

Aigang is a blockchain-based insurance protocol that aims to investigate and create digital insurance prototypes that are powered by blockchain. It would allow the community, businesses, and developers to develop insurance prediction markets and insurance products. Aigang is based in Singapore and was founded in 2017 (Salmon, 2017). The objective is to develop a smart contract-based system with risk-based tokenization that will serve as a self-

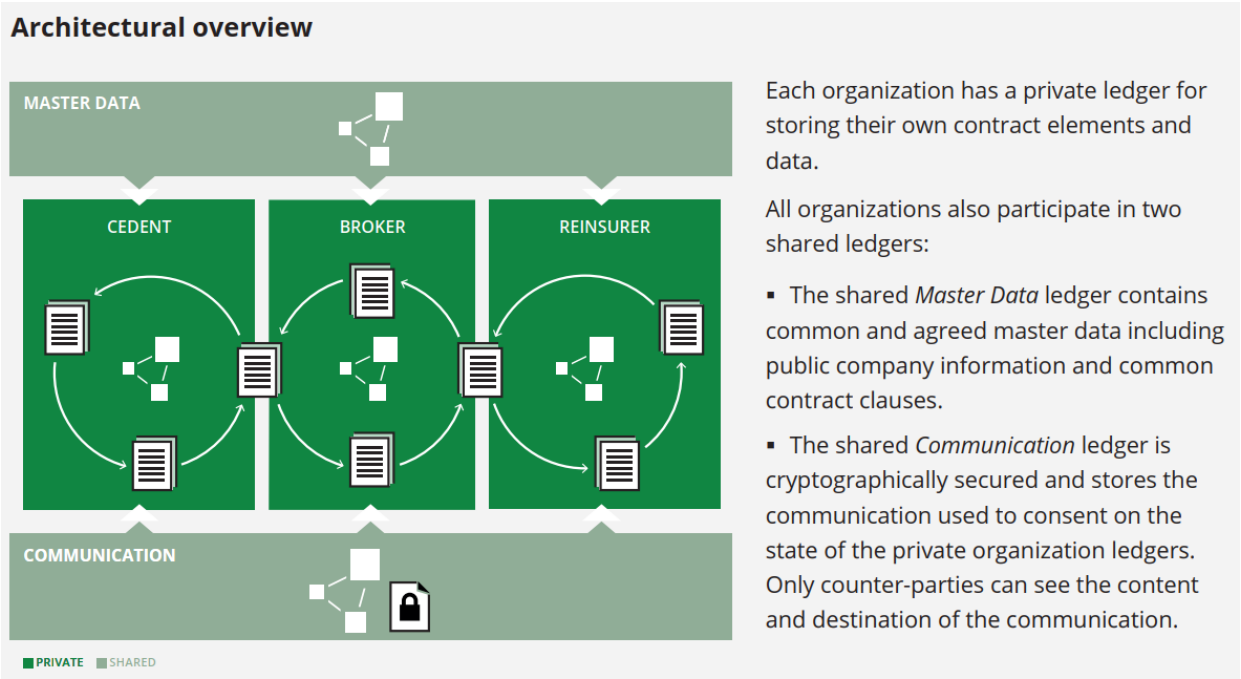
insurance platform for any manufacturer or insurance provider (Chen, Xu, Shi, Zhao & Zhao, 2018). The Aigang Network's blockchain, which employs Decentralized Autonomous Organization (DAO) and smart contracts, delivers next-generation digital insurance for Internet of Things (IoT) devices (Salmon, 2017). They use smartphones for testing their blockchain protocol for digital insurance. The biggest challenge is the battery life on smartphones, warranty periods have decreased and there is an increase in costly repairs and battery replacements. Aigang uses software that assesses the risk and monitors the battery life deterioration. When the battery hits a critical level, the contract is activated and executed automatically, the payout is made. This demo app demonstrates that digital insurance for IoT devices is possible with new technology (Salmon, 2017).

Lemonade is “a startup that offers homeowners and renters insurance powered by artificial intelligence, blockchain, and behavioural economics” (StartUs Insights,2021). They handle claims employing artificial intelligence and chatbots. An example is that Lemonade utilizes videos generated by policyholders to assess the legitimacy of a claim, and it is reported that claims have been paid out in as little as three seconds. According to the CEO of Lemonade, expenses in the insurance industry could be cut by a factor of ten. He also notes that the expense ratios in homeowner's insurance are to blame for roughly a third of premiums and loss adjustment charges, which make up 10–12% of premiums. He believes that by cutting expenses and employing alternate techniques of claims adjustment, P2P insurance systems such as Lemonade, customers' premiums could be reduced (Salmon, 2017). The company is a public benefit organization with a unique business model that includes donating a part of its underwriting revenues to a charitable organization selected by each client upon enrolment (Wikipedia, 2021).

At last, we should also mention B3i's prototype - known as Codex 1. The goal of Codex 1 is to automate catastrophic reinsurance operations. Insurers, brokers, and reinsurer companies will all be gathered on the same blockchain. In the Figure below we can see an architectural Overview of Codex 1.

The significant consumer benefits from DLT-facilitated P2P insurance are starting to become more visible despite some potential regulatory challenges. Salmon's 2017 Report argues that the NAIC has acknowledged that P2P insurance as a business model is currently being offered using conventional technology and that DLT might make it even more open and credible for customers because it is not governed by a central authority. Consumer savings and enhanced consumer satisfaction can be achieved by streamlined claims handling combined with a reduction in claims adjustment costs (Salmon, 2017).

Figure 11: Architectural Overview of Codex 1



Source: Alessandri (2018).

3 RISKS AND CHALLENGES

When it comes to adopting any new technology, different challenges and risks need to be considered (Popovic et al, 2020). How far and how fast blockchain will develop is dependent on laws and regulations, technology itself, business strategy and culture, processes, and financial costs. It is also important to define what regulatory approaches are needed to balance its ingenuity versus the potential for unintended systemic risks to the financial system (Brophy, 2019). In order to provide confidence in financial markets and assure that everyone follows the rules, blockchains and DTLs rely on collaborative governance. However, this may not be the perfect solution because due to the lack of strategic governance to establish a set of rules and enforce compliance, blockchain has been linked to cybercrime. When blockchain governance is established through policies, procedures, mechanisms, and enforcement rules, the true benefits of this technology may be realized (Yeoh, 2017). Furthermore, there is a lot of focus on the potential possibilities and benefits in published research about blockchain, but there is a need to examine if the actual use is possible and what are the main challenges that this technology is facing. The business model of insurance companies demands a big amount of administration for policyholders, underwriting, claims processing, and regulatory affairs. As we discussed earlier, there are theoretical examples of how blockchain can improve insurance processes, but actual examples in action have yet to come to life. Another consideration made by Brophy in the 2019 report is that in the

insurance industry which is highly regulated on a national and international level, regulators have a key function in the adaption of any new technology in the industry. Moreover, a lot of concern is being expressed regarding the use of blockchain due to the instability and vulnerabilities linked to virtual currencies and their trading, which has become the primary concern for government authorities around the world (Yeoh, 2017). Thus, in addition to this, before applying this technology to the insurance industry, it is important to define what kind of innovation this technology brings to the business, the function of it that will allow insurance companies to operate, as well as real-time examples of this application. As mentioned in Brophy (2019), it is very important to research what is the attitude of the insurance industry and regulators toward blockchain applications in insurance. On the other hand, each company needs to analyse their business and what improvements could blockchain bring to their business. Companies should take a look at the limitations of this technology, examining its scalability, security, and standardization. Under which conditions the implementation of blockchain is optimal. For example, if the transaction involves multiple parties and requires a precise and immutable record, blockchain represents a good solution. Also, if there is an incentive to manipulate the data for competing advantages, or use the same asset multiple times. On the other hand, the insurance industry players should continue to operate under the current transaction model if the transactions only involve a small number of parties, don't require an intermediary, or are already handled by a reliable intermediary (Lorenz et al., 2016).

3.1 Cost of Adoption

Blockchain can be a disruptive technology and challenging to implement, especially in a commercial sense. As mentioned in the 2016 Deloitte report the aggregated cost for peer-to-peer transactions is very high and it varies from one type of blockchain to another. This high cost comes from inefficiency because each node conducts identical actions on its own copy of the data as every other node while trying to be the first one to find a solution. In the case of Bitcoin, for example, the overall operating expenses involved with validating and distributing transactions on the public ledger are projected to be $600 million or higher per year, not considering the price of procuring specialized mining hardware. This leads to a question of how much productivity increases for the whole network, how many nodes it takes to reach its full potential and there is also the question of the nodes that work diligently but make a smaller contribution to the overall network. Therefore, we can say that the implementation of blockchain, either in individual processes or sector-wide has to be studied thoroughly and analysed from the perspective of how much value is added to the consumers or sectors at large (Grewal-Carr & Marshall, 2016). Another consideration regarding the cost of adopting this technology is related to the lack of talent. Blockchain solution creation is a field in which abilities in mathematics, cryptography, economics, data structure, and computer science intersect. It is uncommon to find skilled developers that match all of the criteria. Even more difficult is to find a person with all the mentioned skills that additionally have knowledge of the insurance industry (Popovic et al., 2020). Global demand for

blockchain engineers has increased drastically from 2019 to 2020 by more than 517% (Sharma, 2020). The lack of talent represents one of the reasons why the development of this technology has a slow pace. Despite being in high demand it is really difficult to find developers who understand the processes behind the blockchain, and if we add the required knowledge of insurance industry processes this does represent a big obstacle for future growth. On the other hand, there is also a problem of scale. In the case of permissionless blockchains, the full benefit is only reached in the network effect. So far only cryptocurrencies have this level of scale. On the other hand, in the case of permissioned blockchains, there are selected few who own intellectual property (IP), this could be a barrier for other participants to join the network, thus hampering the adoption. At last, as this technology is still in the making, standards/platforms are constantly emerging. Blockchain has gained a lot of popularity these recent years, but its development doesn't follow the hype, it will take time for this technology to grow, become cost-effective for broad use, and, most crucially, be tested in real-world settings (Popovic et al., 2020).

3.2 Security

Blockchain relies on cryptography and consensus mechanism to replace the trusted centralized authority (Popovic et al., 2020). Many possible blockchain applications need smart contracts and all transactions to be linked to a known identity. This is not the case with, for example, cryptocurrencies that offer pseudonymity and link transactions to ‘wallets’, not individuals, this raises an important question about the privacy and security of data stocked on a distributed ledger. On the other hand, blockchain represents secure encryption and decentralized architecture and the identities created on it are distinctive and provide a high level of trust that the participant is whom they claim they are. This doesn’t take away the need for each organization to make a specific design for the need for privacy and security concerns (Grewal-Carr & Marshall, 2016).

In the last few years, there have been some potential security concerns in the application of this technology. One of these concerns is a 51% attack, this is a method aimed at breaking blockchain for double-spending. This means that attackers with 51% of the computing resources can overturn the transactions in the alternative block on a side chain or branch and conceal what is happening in the blockchain's main chain (Islam et al., 2021). This ability to modify the transactions can lead to a double-spending attack.

One more difficulty is related to the immutability of blockchain, as useful as it is; it can be a doubtful advantage as well. This implies that any type of blockchain hack, fraud, or error cannot be rectified without severe actions. The blockchain is "hard-forked" in this situation, which creates a permanent disagreement and makes the new and old copies of the blockchain incompatible (Popovic et al., 2020).

Humans are developing all the software-based solutions and human action is not error-free. This means that coding errors can lead to threats to blockchain applications. Blockchain is

an open platform which means that anyone can join, including hackers that can take advantage of coding errors. Hackers stole $55 million worth of Ether digital money in 2016 by taking advantage of programming flaws in the Distributed Autonomous Organization (DAO) platform (Islam et al., 2021).

Another issue that has arisen is involving external data that is not coming from the blockchain but from the outside world i.e. data that is not produced within the blockchain. As an example, we have smart contracts that often have external data feeds from sources known as “oracles” (i.e. off-chain data). These oracles are data silos that operate in a centralized way. This makes them susceptible to attacks because smart contracts are insufficiently "smart" to judge the accuracy of data feeds. This exposes smart contracts to inaccurate external data feeds, which is one of the biggest barriers to the widespread adoption of blockchain and smart contracts in practical applications (Popovic et al., 2020). These considerations of privacy surrounding ideas of value, safety, and integrity are critical for gaining public acceptance of blockchain (Grewal-Carr & Marshall, 2016).

3.3 Regulation

It has been always a challenge for regulators to keep up with the advances in technology. Blockchain wants to completely tackle inefficiencies in the conventional intermediated system and existing regulations are made for this centralized governance structure. One of the main motivations and goals of this new technology is to reduce oversight, but these centralized systems have acted as shock absorbers in times of crisis, so even though this technology will reduce oversight this decentralized system would be much less resilient to shocks. This means that shocks can impact participants directly, there is a need for careful design and additional clarity in the application of this technology. The necessity for an undisputed and coherent interpretation of regulations, particularly concerning the regulatory perimeter, customers' onboarding, risk management, and consumer protection, may cause a delay in the expansion of blockchain solutions (EIOPA, 2021). So far there haven't been a lot of activities related to these regulating barriers, the innovation facilitators are still focused on the discussion about possible developments in the application of this technology, building a technical capacity, and identifying the risk that comes from its application. Even though the scope of these innovation facilitators depends from country to country, they could be more focused not just on entities that want to launch blockchain solutions but also to improve the dialogue between market operators when creating a new service, discussing possible standards and removing regulatory impediments. For now, this dialogue is mostly conducted with companies that plan to use new technologies such as blockchain. Thus, there is a compelling case for blockchain applications to operate within current regulatory frameworks rather than outside of them, but this demands that regulators across all industries comprehend the technology and its effects on the companies and consumers in their industry (Grewal-Carr & Marshall, 2016). Security and privacy, governance, scalability, and standardisations

are key problems and hazards to consider in the context of existing regulatory frameworks (Tarr, 2018).

As Yeoh's (2017) report elaborates, in the digital environment we have regulations that control activities in the form of legal codes and technical codes. Legal codes ensure compliance by following the rules that can be broken, which means that when rules are broken, errors are handed back, no activity takes place, and compliance is guaranteed. Technical codes are more rigid, which means that they follow the rules even when compliance results in unfavourable or unexpected outcomes. Legal and technological codes control today's contemporary financial system. In blockchain, technical codes are the only means of defining and implementing the rules. Participants only have to use compliant software, which lowers costs. Until now, the financial system has relied on legal codes that include governance or private regulation (for example Visa Core Rules) or regulation exemplified by statutory oversight of for example Bank of England. Public legal codes would have to govern blockchain, and policymakers would have to take into account all micro- and macro-prudential aspects.

Blockchain has struggled with formal governance mechanisms since now it is mostly governed by ad hoc processes made by a few institutions and power brokers. Its goal is to design formal governance respecting its anti-institutional character. This arises the big question of whether the technical codes would be enough to reach the desired level of formal governance and if technical codes can indeed replace the legal codes and reach the optimal outcome. The owner of a permissioned distributed ledger has unambiguous legal and technical control over the code. This could also be useful in the repression of criminal activities and tax fraud. For regulators, it is especially important to make sure the operating system can withstand recurring risks and market failures. This indicates that the distributed ledger could also be regulated by legal and technical codes. In the case of premissioned DTL, this means an imposing legal obligation on the proprietor, and in the permissionless systems, legal codes should ensure compliance, which has shown to be more complicated to regulate. One example of how this problem is tackled is BitLicense which provides digital currency services. BitLicence functions in the following way, although the technical code for the ad hoc process is supplied by private participants, the technical codes, which include software and protocols, can come from the public sector. As a result, there is a chance that technical codes will be partially public and will be seen as being regulated by the public regulation of technical codes as opposed to legal codes. The implication could be the following, the technical codes could have a public standard for the code. A development like this one could lead to the fulfilment of the regulatory goals and reduce the requirements for the legal codes to regulate the system. Furthermore, the permissioned system could be built in a way that enables the public regulators to impact the flow by combining legal and technological codes, rather than only legal codes, as is now the case (Yeoh, 2017). This new technology is changing the current laws and the approaches to regulation. New and expanding applications of blockchain would require an adaptation of the existing combined with the new legal codes. The supporters of the idea of a decentralized system where information and interaction are

free of centralized authority advocate that this is the future. Another view is that regulating blockchain at such an early stage could be counterproductive, as technology is still emerging and changing its shape and purpose putting regulation on top of it could stop it from reaching its full potential. Following this logic, it is still early for the regulators to intervene, a better solution would be to find a new approach within the existing framework, and not make new rules that can repress the development of the technology. There is also a challenge regarding the adaptability of the existing framework. Another important distinction that needs to be made is that regulation is different from governance. Past experience shows that good governance is a better solution than strict regulation to keep a healthy and functioning environment. Another consideration is that also bottom-up governance is a better option than top-down regimes of control. In addition to the existing system, this type of governance could enhance market participants' behaviour by increasing transparency and civic engagement (Tapscott & Tapscott, 2016).

When we talk about blockchain applications in the insurance industry, international regulators seem to support this idea. They see a big opportunity in its use in commercial lines, the reinsurance business and intra-group transactions (EIOPA, 2017). The International Association of Insurance Supervisors is monitoring blockchain insurance applications and has raised concerns about data ownership, solvency, clarity, the use of smart contracts, and other issues (IAIS, 2017). EIOPA (2017) attempted to define the concept of peer-to-peer insurance, taking into account the numerous versions of peer-to-peer insurance applications, as well as the various types of claims processing and premium handling. National regulators have expressed an interest in this technological innovation in insurance known as InsurerTech. Some of the European regulators have tested this concept in a controlled environment so-called ‘sandbox’ concept, where with enhanced regulatory control, this technology is evaluated under specific regulator-imposed conditions. There are two points of view on this sandbox concept. The first is a technical perspective, which provides a fluid and expressive thinking atmosphere which supports both impromptu and more formal analytical tasks. The second view is the regulatory view, it exempts particular businesses or activities from regulation where this concept is temporary, limited in scope, and not permanent. Despite its flaws, the sandbox approach is the most suitable for the examination of blockchain applications in the insurance industry. Another approach could be ‘innovation hubs’. The idea behind innovation hubs is to offer general advice to firms throughout the process, provide a better understanding of rules and supervisory processes and quick access to the market. FinTech testing models are more focused on the innovation hubs compared to the other evaluation models. However, some regulatory authorities have started to consider some other evaluation techniques, for example, Australia is using both sandbox and innovation hub techniques to encourage the development of new technology in FinTech (Brophy, 2019).

DLT has disrupted the world since its first appearance in 2008 and it is here to stay. The regulatory position concerning this new technology is still evolving and regulators all over

the world are examining the potential effect of this new technology on the sector of financial services.

Regulators over the world are taking some action in order to address the regulative perspective of the blockchain adoption process. For example, regulators in the UK have issued DP17/3, basically inviting public comment on the possible future advancement of DLT in the markets they regulate. The collected and sorted feedback will be published in the Summary of Responses or a new Consultation Paper. In France, there has been some interest in the new technology but, there haven't been any major initiatives yet. In 2016, the government authorized the distribution of debt-based products on a ledger. In 2017, there have been several hearings about DTL and its legal and social issues or regulations held by the Prime Minister's cabinet for national strategies. More recently, a working group has been set up to assist the government in determining which initiatives they will have to guide in the DTL application. This group was formed by a French institution dedicated to the development of the French financial sector. Still, there haven't been any real DTL experimentations, only conferences and workshops.

On the other hand, the German regulator, BaFin has recognized the influence DTL and blockchain could have on the financial sector. The President of BaFin, Felix Hufeld in his speech at the G20 in 2017 said that regulation should take a neutral attitude towards digital processes and not discriminate against them. New risks are emerging from digitalization processes for the overall stability and consumers, but on other hand, there are considerable opportunities this technology offers. He said that the biggest challenge is to get the timing right, meaning that regulation should allow new technology to develop its potential without any regulatory constraints that might hurt its growth, but regulators must always be aware of potential threats to financial stability and make sure that thought by previous experience act proactive if they see a sign of new global crisis emerging (Salmon, 2017).

In terms of EU regulation, the European Parliament approved DLT's "smart regulation" in 2016. German MEP Jacob von Weizäcker said that they prefer precautionary surveillance over post-regulation to avoid restricting innovation. In a report released in 2017, ESMA argued that the short-term application of DTL is not obstructed by the current EU regulatory framework and that there is no need for regulatory action because DTL is still in its early stages. Later that year, the European Commission formed a 'European Union Blockchain Observatory' to build knowledge on areas such as infrastructure, governance and validation mechanisms, contracts, regulatory and legal difficulties, scalability, and standardization, as well as to investigate potential use cases inside the EU (Salmon, 2017). #The 'Blockchain4EU Project' was formed to assist industrial use applications for blockchain and DLT. EIOPA has also played an active role in the DTL debate, hosting the first InsurTech round table. The main conclusion of the round table was that private blockchains require less supervision. Supervisors in public blockchains can have to pay attention to a variety of different things, such as the key function of miners and nodes or difficulties with security

and privacy. Some attendees also suggested that regulatory authorities look into removing some of the statutory impediments to blockchain deployment (Salmon, 2017).

Meanwhile, in the United States, the Financial Industry Regulatory Authority (FINRA) published a paper titled "Distributed Ledger Technology: Implications of Blockchain for the Securities Industry." The paper's purpose was to start a conversation with market players on the usage of DLT in the securities industry. The NAIC established an Innovation and Technology Task Force that should serve as a forum for regulators to educate themselves and discuss innovation and new technology, monitor new developments in this field and how is this affecting the current regulatory framework and develop new regulatory guidance (Salmon, 2017).

3.4 Business Strategy and Culture

Blockchain is a technology that will bring the most value to companies if the companies collaborate, due to the effect of the game theory that is in place. Companies need to both cooperate and compete in the network to benefit from this technology. The problem with the current approach is that organisations are mainly developing their blockchains and applications within organizations. This contradicts the main purpose of DTLs which requires a network structure and is more efficient on a larger spectrum. Another problem within the organisations is that by applying this technology the organisation loses control; trust and authority reside in a decentralized network rather than in a strong centralized institution. According to estimates, a blockchain involves 80% transformation of business processes and 20% technology implementation (Grewal-Carr & Marshall, 2016). This requires a more elaborative plan focused on the comprehension of opportunities and changes that this technology brings to the business model of every organisation. Some of the struggles that companies will face are the following:

- The first risk is the possibility of disclosing commercially sensitive data, which could result in a loss of competitive advantage. As a result, businesses are reluctant to engage in business transactions on a public, permissionless blockchain. A so-called ZKP is attempting to resolve this issue. ZKP is an encryption method that enables one party (the prover) to demonstrate to another party (the verifier) that they are aware of a value x without disclosing any additional information. In other words, ZKP permits data sharing between two parties without disclosing the content of the data, potentially enabling private transactions on open, permissionless blockchains.

- Secondly, there is a natural aversion to change, new technology frequently brings the need for a change of mindset and existing processes. In order to have a successful implementation of new technology, the organisation needs to create a culture that encourages innovation and continuous improvements. A good technique would be to

transform in a gradual and ringfenced manner, such that companies create a new brand under the parent company (Popovic et al., 2020).

4 IN-DEPTH INTERVIEW ANALYSIS

As already mentioned in the Introduction, this master thesis is trying to answer three main questions, the first one is to investigate the wider impact of blockchain on the insurance industry, the second one is to investigate the possible use cases and the last one is to present the main obstacles this technology is facing. An In-depth Interview Analysis should further give an insight into these questions by interviewing industry experts who possess in-depth knowledge of insurance company policy implementation and decision-making skills. My interlocutors are VP of Business Development in VouchForMe, Aleš Tomažin and CEO of Adacta Slovenia, Boris Bajić.

VouchForMe is built on the idea that insurance can be customized for each individual. Their mission is to create an ecosystem in which community opinion is used to assess risk for individuals, resulting in lower insurance costs. The goal is to make a risk assessment and segmentation smoother for insurance companies to use when developing affordable insurance solutions for end users. Insurance for your car, home, or business. The VouchForMe team is dedicated to changing the insurance industry's traditional approach and is constantly looking for new approaches to insure our customers more quickly, efficiently, and appropriately. The team is made up of experts in insurance solutions, technology, and business intelligence. Aleš Tomažin is the VP of Business Development at VouchForMe. Aleš has 15 years of diverse experience working in the highest position of leadership in the insurance industry. He is a prominent member of the blockchain community and holds a PhD in Actuarial Science (VouchForMe, 2020).

Adacta is one of the top software developers for the insurance sector. AdInsure, their insurance platform, offers Life and P&C insurers a reliable way to modernize their procedures and workflows. Since its founding in 1989, Adacta has worked with insurance companies to develop their digital capacities and generate new revenue. Their mission is straightforward: to use technology to help future industry leaders achieve their full potential. In April 2020, Adacta appointed Boris Bajić as the CEO of Adacta Slovenia. Previously Bajić was a member of the management team, he was also responsible for overseeing the everyday operations of the business analysis team as the Head of Business Analysis, as well as product development in his role as the Chief Product Officer. As a certified actuary working for the insurance regulator, he gained experience and a deep understanding of the insurance industry which translates into a better understanding of Adacta customers (Adacta Fintech, 2022).

4.1 Discussion and comparison analysis

The primary objective of this master's thesis is to examine the potential influence of blockchain on the insurance business and to investigate possible use cases. In-depth interviews are utilized as a method for further research based on the viewpoints of Slovenian experts, as well as drawing parallels with the Yu, Wang, Tseng, and Tsao study from 2021.

We can start with the view of the experts on their opinion about this technology. All of them seem concordant that this is a new, emerging technology that has potential. Decentralization is pointed out as one important change this technology may bring, but also the instability of cryptocurrencies is a big problem that makes others reluctant to embrace this new technology.

Regarding the future trends in insurance companies, the experts from the 2021 paper see the insurance industry moving towards an increase in data sharing between insurance companies and reduction of costs and efficiency improvement, but not necessarily through blockchain. When asked about the implementation of blockchain in insurance primary benefits are seen in identity verification and recognition. On the other hand, Mr Tomažin sees that the future of claim handling and payment procedures is definitely in blockchain, while Mr Bajić is not convinced that blockchain will disrupt the insurance sector. He believes that insurers will find their way to use all the advantages of the latest technologies but in the end, the core business of insurance will stay the same - taking a portion of your risk for a proper price.

Smart contracts and their application were discussed in both papers and the main conclusion can be drawn from the answers. They are quite prudent about smart contracts, some of the reasons are that it is hard to combine the old (traditional) and the new (blockchain) data, further that it is hard to decentralize insurance, then the complexity of insurance contracts could also be problematic. Potential is seen in combination with IoT to provide a better level of automatization, also it could highly beneficial for intellectual property rights, owners' identity and fraud reduction. Furthermore, a big benefit is seen in the immutability of the data, that the data can not be modified. Mr Tomažin believes that smart contracts have already started to change the banking industry and payments and that it has the potential to do the same for the insurance industry. Mr Bajić on the other hand thinks that blockchain is more suitable for banking than for insurance because of the sole nature of the contracts, more specifically of the „promise" within the contract.

In the end, when ask if they use blockchain in their companies, only two of the experts use it to some extent but say they are still too early in this technology. Mr Bajić and Adacta have shifted more towards AI and Machine Learning which they believe lies far greater benefit for their current and future customers, than in blockchain.

After summarizing, we can analyse three main points from the interviews.

Firstly, As we can see from both interviews, experts are quite cautious when talking about blockchain and its use in the insurance business. Maybe it is because of the frigid form of business in insurance, but that should not be an obstacle to investigating the possible ways to improve and digitalize the processes by using this innovative technology. Blockchain is still in its early phases and there is a lot to be examined about its real application and the understanding of how it works is limited. I think that experts could agree that blockchain has great potential in the insurance business. The views on how it could be used are different, but all of them see a way that blockchain could improve the insurance business. Of course, we must also mention that the insurance business is something that exists for a very long time, they have always operated throughout all the different changes that society went through. They did adapt and change in accordance with the new conditions, but it never disrupted the insurance business. Maybe this is why they are not eager to use this new technology and jump on the front line to test the new blockchain applications.

Secondly, I think that all the interviewed parties do see some potential in the use of this technology, which insinuates that there is a real benefit for the insurance companies to start exploring the adequate application of this technology in their businesses. Their perspective of application is different, but the main conclusion is the same. I would say that the main challenges would be the regulatory concerns, which were further discussed in Chapter 3. Also, the complexity of insurance contracts is another big obstacle, like Mr Bajić already said, no one is questioning if the contract was signed, but the sole nature of the „promise" within the contract. The primary difficulty that this technology has to solve before it can be used widely in the insurance industry is the legal validity, how to decide in the event of a dispute, or how to incorporate various legal difficulties.

Thirdly, This master thesis is trying to examine the real potential and limitations of this technology. Also, the goal is to start the conversation about the possibilities and new technologies like blockchain that arise in recent years. To make people wonder and inspire them to step away from traditional thinking. I think that the insurance industry is starting to realize the potential of blockchain, a clear sign is the creation of the B3i initiative. On the other hand, because of financial organizations' conservative character and demand for stability and reliability in their operating systems, I also believe that they won't become pioneers in implementing new technology. This is a whole new type of software, in early development and has already experienced its share of failures, all of this makes the adoption process much slower (Williams, 2017). I believe the "blockchain linked with insurance" paradigm has a future and will be utilized at higher levels and over a larger spectrum in the insurance business. Additionally, when blockchain is used in conjunction with legislative regulations, it will significantly contribute to the real economy and the reduction of financial risks.

CONCLUSION

This master thesis provides insight into understanding, assessing and adopting blockchain in the insurance industry. It discusses the unique characteristics of blockchain and smart contracts, potential uses that are currently being developed, hazards, and difficulties related to blockchain adoption in the insurance industry. The insurance industry is very prudent and frigid, but that should not be an obstacle to investigating the possible ways to improve and digitalize the processes by using this innovative technology. Although, this technology is still in its infancy and blockchain is yet to have a significant influence on the insurance business, it has the potential to be very beneficial for the industry. The adoption of technology, like in the case of most innovations, does not occur overnight. I believe that there are enough indicators that suggest that blockchain could bring real benefits to insurance companies, which should be an incentive for insurers to start exploring the adequate application of this technology in their businesses. Commercial insurance will become more distributed, and more artificially intelligent (Saxena & Kumar, 2021). Blockchain together with IoT and AI would lead to changes in traditional insurance business models. However, there are several technical issues with blockchains that need to be taken into account. The truth remains, that with blockchain or with alternative use cases, blockchains are paving the way to innovative solutions that will be deployed in the future of the insurance business. Some use cases are simpler and easier to implement, while others are risker, especially considering the risk-reward relation. The range of options is vast, and the insurance business will need time to adapt and respond. Most importantly, all industry participants must choose the use case that will be most advantageous to them. Moreover, blockchain adoption is something that requires the collaboration of multiple stakeholders. Some industry leaders have realized this and that is how the B3i initiative was formed. Governments and regulators should also join in this innovative research in order to provide regulatory clarity for blockchain. Applications and use cases for blockchain in insurance will develop over time, and acceptance will rise as attitudes change, altering current insurance business and operational structures (Popovic et al., 2020). I believe that blockchain's mostly unexplored potential will start to emerge as new and developing technologies are regularly implemented inside the insurance sector. In comparison to artificial intelligence, robotic process automation, and big data, blockchain is definitely still in the early stages of adoption. Insurers that invest in blockchain now will gain a significant first-mover advantage, which should be taken into account while developing their digital ecosystems. Given the recent explosion of blockchain-enabled technology like Bitcoin and the speed at which the insurance industry is undergoing a digital transition, I believe blockchain will have a profound impact on the sector in the years to come. New technologies will alter the insurance industry as we know it. The degree and nature of the interruption remain to be known. However, it appears that InsurTechs will become more prominent as digital innovation in the insurance business unfolds (Lynn, Mooney, Rosati, & Cummins, 2019).

REFERENCE LIST

1. Abdikerimova, S., & Feng, R. (2021, September 23). *Peer-to-peer multi-risk insurance and Mutual Aid*. European Journal of Operational Research. Retrieved October 9, 2022, from https://www.sciencedirect.com/science/article/abs/pii/S0377221721007761?via%3Dihub

2. Adacta Fintech. *About Adacta l Life and Non-life insurance software platform.* Adacta. (n.d.). Retrieved October 9, 2022, from https://www.adacta-fintech.com/about-us

3. Aggour, K. S., Bonissone, P. P., Cheetham, W. E., & Messmer, R. P. (2006, September 15). *Automating the Underwriting of Insurance Applications*. AI Magazine, 27(3), 36. https://doi.org/10.1609/aimag.v27i3.1891.

4. Alessandri, E. (2018, February 16). *B3i Codex1 Demo. InsureTech - Europe Chapter of the CPCU*. Retrieved October 9, 2022, from https://europe.cpcusociety.org/system/files/docs/public/02-Europe%20Chapter%20Meeting%2016%20Feb%202018-Enrico%20Alessandri-B3i%20Codex1%20Demo.pdf

5. Alharby, M., & Moorsel, A. V. (2017). *Blockchain-based Smart Contracts: A Systematic Mapping Study*. Computer Science & Information Technology (CS & IT), 125-140. doi:10.5121/csit.2017.71011.

6. Banton, C. (2022, September 27). *Insurance underwriter: Definition, what underwriters do*. Retrieved October 9, 2022, from https://www.investopedia.com/terms/i/insurance-underwriter.asp

7. Bramblet, J. (2020, August 11). *Ultimate Guide to Blockchain in Insurance.* Retrieved October 9, 2022, from https://insuranceblog.accenture.com/ultimate-guide-to-blockchain-in-insurance

8. Brophy, R. (2019). Blockchain and Insurance: A review for Operations and Regulation. Journal of Financial Regulation and Compliance, 28(2), 215-234. doi:10.1108/jfrc-09-2018-0127.

9. Calcaterra, C., Kaal, W., & Rao, V. (2019, June 13). *Decentralized underwriting*. Retrieved October 9, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3396542

10. Cao, B., Li, Y., Zhang, L., Zhang, L., Mumtaz, S., Zhou, Z. & Peng M. (2019, July 10). *When Internet of Things Meets Blockchain: Challenges in Distributed Consensus*. IEEE Network, vol. 33, no. 6, pp. 133-139, Nov.-Dec. 2019, doi: 10.1109/MNET.2019.1900002.

11. Cao, S., Lyu, H., & Xu, X. (2020, September 07). *InsurTech development: Evidence from Chinese media reports*. Technological Forecasting and Social Change, 161, 120277, ISSN 0040-1625. doi:10.1016/j.techfore.2020.120277.

12. Carolin, J. (October 2019). *B3i Factsheet.* B3I factsheet - mapfrere.com. (n.d.). Retrieved October 9, 2022, from https://www.mapfrere.com/media/b3i-factsheet-1.pdf

13. CB Insights. (2022, July 19). *How blockchain is disrupting insurance*. CB Insights Research. Retrieved October 9, 2022, from https://www.cbinsights.com/research/blockchain-insurance-disruption/

14. Chekriy, S. & Mukhin, Y. (2018, May). *Blockchain Platform for Insurance-related Products*. The Glass Cube Group. Retrieved October 9, 2022, from https://policy.report/Resources/Whitepapers/84a2f92f-e48b-40eb-98b0-a17f39a642dc_i-chain.net.wpaper_rev_005.pdf

15. Chen, C., Deng, Y., Tsaur, W., Li, C., Lee, C., & Wu, C. (2021). *A Traceable Online Insurance Claims System Based on Blockchain and Smart Contract Technology*. Sustainability, 13(16), 9386. doi:10.3390/su13169386.

16. Chen, W., Xu, Z., Shi, S., Zhao, Y., & Zhao, J. (2018, December). *A survey of blockchain applications in different domains*. In Proceedings of the 2018 International Conference on Blockchain Technology and Application (pp. 17-21).

17. Chen, X., & Zhang, X. (2019). *Secure electricity trading and incentive contract model for electric vehicle based on energy blockchain*. IEEE Access, 7, 178763-178778. doi:10.1109/access.2019.2958122.

18. Cohn, A., West, T. & Parker, C. (2017). *Smart After All: Blockchain, Smart Contracts, Parametric Insurance, And Smart Energy Grids.* Georgetown Law Technology Review, 1:2, 273–304. Retrieved October 9, 2022, from https://perma.cc/TY7W-Q8CX.

19. Cong, L. & He, Z. (2019). *Blockchain Disruption and Smart Contracts*. The Review of Financial Studies, 32(5), 1754-1797.

20. ConsenSys (2021). *Blockchain in Insurance: Use Cases and Implementations*. Retrieved October 9, 2022, from https://consensys.net/blockchain-use-cases/finance/insurance/

21. Crosby, M., Nachiappan, Pattanayak, P., Verma, S., Kalyanaraman, V. (2015, October 16). *BlockChain Technology, Beyond Bitcoin*. Sutardja Center for Entrepreneurship & Technology Technical Report. Retrieved October 9, 2022, from https://scet.berkeley.edu/reports/blockchain/

22. Crunchbase (2017). *InsureX Technologies - Crunchbase Company Profile & Funding*. Retrieved October 9, 2022, from https://www.crunchbase.com/organization/insurex-technologies

23. Cultu, D., Ganjani, K., Larrea, E., & Müssig, M. (2022, May 4). *Claims 2030: Dream or reality?* McKinsey & Company. Retrieved October 9, 2022, from https://www.mckinsey.com/industries/financial-services/our-insights/claims-2030-dream-or-reality

24. Derebail, A. (2018, March 13). *Three areas in the insurance industry to use blockchain IBM Supply Chain and blockchain blog*. IBM Supply Chain and Blockchain Blog. Retrieved October 9, 2022, from https://www.ibm.com/blogs/blockchain/2018/03/three-areas-in-the-insurance-industry-to-use-blockchain/

25. *DP17/3: Discussion paper on distributed ledger technology - FCA*. Financial Conduct Authority. (2017, April). Retrieved October 9, 2022, from https://www.fca.org.uk/publication/discussion/dp17-03.pdf

26. EIOPA (2021). *Discussion paper on blockchain and smart contracts in insurance*. Luxembourg: Publications Office of the European Union.

27. Fuchs, P. (2019). *Blockchain: Everything you need to know about how this remarkable technology will impact you, your organization and society*. Retrieved October 9, 2022, from https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2019/jan/gl-2019-blockchain-101-overview-mercer.pdf

28. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018, February 20). *Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?* Future Internet, 10(2), 20. doi:10.3390/fi10020020

29. Geroni, D. (2022, August 15). *Top 5 Blockchain Security Issues in 2022*. Retrieved October 9, 2022, from https://101blockchains.com/blockchain-security-issues/

30. Grima, S., Spiteri, J., & Romānova, I. (2020). *A steep framework analysis of the key factors impacting the use of blockchain technology in the insurance industry*. The Geneva Papers on Risk and Insurance - Issues and Practice, 45(3), 398-425. doi:10.1057/s41288-020-00162-x.

31. Hemanth, J., Fernando, X., Lafata, P., & Baig, Z (2018, August 8). *International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018*. (1st ed.). Springer Cham. doi:https://doi.org/10.1007/978-3-030-03146-6.

32. Henry, K. & Hogan, B. (2018, February 16). *Insurance and blockchain: What policyholders need to know?* Retrieved October 9, 2022, from https://www.bradley.com/insights/publications/2018/02/insurance-and-blockchain-what-policyholders-need-to-know

33. Huang, J., Kong, L., Chen, G., Wu, M., Liu, X., & Zeng, P. (2019, March 06). *Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism*. IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3680-3689, June 2019, doi: 10.1109/TII.2019.2903342.

34. IBM (2021). *What are smart contracts on blockchain?* Retrieved October 9, 2022, from https://www.ibm.com/topics/smart-contracts

35. International Association of Insurance Supervisors (IAIS). (2017, February 21). *FinTech Developments in the Insurance Industry*. Retrieved October 9, 2022, from https://www.iaisweb.org/uploads/2022/01/Report_on_FinTech_Developments_in_the_Insurance_Industry.pdf

36. Iredale, G. (2022, August 15). *History of blockchain technology: A detailed guide*. Retrieved October 9, 2022, from https://101blockchains.com/history-of-blockchain-timeline/

37. Islam, M. R., Rahman, M. M., Mahmud, M., Rahman, M. A., Mohamad, M. H., & Embong, A. H. (2021, Avgust 7). 2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC), 2021, pp. 227-232, doi: 10.1109/ICSGRC53186.2021.9515276.

38. Kim, H. & Mehar, M. (2019, November 21). *Blockchain in Commercial Insurance: Blockchain Research Institute ™*. Retrieved October 9, 2022, from https://www.blockchainresearchinstitute.org/project/commercial-insurance/

39. Kleber, U. (2019, July 23). *Blockchain on the block – interview with prof. dr. Sandner, Frankfurt School of Finance and Management*. Retrieved October 9, 2022, from https://www.the-digital-insurer.com/blockchain-on-the-block-interview-with-professor-dr-sandner-frankfurt-school-of-finance-and-management/

40. Koscielecki, F. (2018, June 15). *Block(claim)chain: A brave new world of claims handling?* Retrieved October 9, 2022, from https://www.ukpandi.com/opinion/blockclaimchain-a-brave-new-world-of-claims-handling/

41. Kot, I. (2020, February 14). *Blockchain in Insurance: 3 Use Cases.* Retrieved October 9, 2022, from https://www.insurancethoughtleadership.com/blockchain/blockchain-insurance-3-use-cases

42. Krause, S. K., Gradstein, H. L., & Natarajan, H. (2019, December 12). *Distributed Ledger Technology (DLT) and Blockchain.* Retrieved October 9, 2022, from https://documents.worldbank.org/en/publication/documents-reports/documentdetail/177911513714062215/distributed-ledger-technology-dlt-and-blockchain

43. Kumar, M. (2020, September 17). *Game-changing potential of blockchain in insurance claims processing*. Retrieved October 9, 2022, from https://blockchain.oodles.io/blog/potential-blockchain-insurance-claims-processing-use-case/

44. Lewis, R., McPartland, J., & Ranjan, R. (2019). *Blockchain and financial market innovation*. J.P. Morgan Center for Commodities at the University of Colorado Denver Business School. Retrieved October 9, 2022, from http://www.jpmcc-gcard.com/wp-content/uploads/2019/03/GCARD-Summer-2019-Chicago-Fed.pdf

45. Lorenz, J. T., Ricciardi, V., Bohlken, N., Olesen, P. B., Higginson, M., & Münstermann, B. (2016, July). *Blockchain in insurance – opportunity or threat?* Retrieved October 9, 2022, from https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-in-insurance-opportunity-or-threat

46. Lounds, M. (2020, July). *Blockchain and its Implications for the Insurance Industry*. Retrieved October 9, 2022, from https://www.munichre.com/us-life/en/perspectives/underwriting/blockchain-implications-insurance-industry.html

47. Lynn, T., Mooney, J. G., Rosati, P., & Cummins, M. (2019). *Disrupting Finance (1st ed.)*. Palgrave Pivot Cham. doi:https://doi.org/10.1007/978-3-030-02330-0.

48. Mainelli, M., & Manson, B. (2016, August 1). *Chain Reaction: How Blockchain Technology Might Transform Wholesale Insurance*. Retrieved October 9, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3676290

49. Marshall, S. & Grewal-Carr, V. 2016. *Blockchain Enigma. Paradox. Opportunity*. Retrieved October 9, 2022, from https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf

50. Meeusen, P. & Sorniotti, A. (2017, November 7). *Blockchain in Re/Insurance, Technology with a Purpose*. Retrieved October 9, 2022, from https://www.swissre.com/dam/jcr:c2213d00-e114-4dde-9782-4bf2e130c892/Presentation_Alessandro_Sorniotti_Paul_Meeusen.pdf

51. Meeusen, P. (2017, September 25). *B3i – Blockchain Insurance Industry Initiative.* Retrieved October 9, 2022, from https://www.swissre.com/dam/jcr:d560374e-d7ba-4472-a28c-1f53f932303b/2017_09_25_B3i_blockchain_insurance.pdf

52. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017, October 5-8). *A review on consensus algorithm of blockchain*. 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2017, pp. 2567-2572, doi: 10.1109/SMC.2017.8123011.

53. Mohanta, B. K., Panda, S. S., & Jena, D. (2018, July 10-12). *An Overview of Smart Contract and Use Cases in Blockchain Technology.* 2018 9th International

Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018, pp. 1-4. doi:10.1109/icccnt.2018.8494045

54. Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019, June 26). *Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities*. IEEE Access, vol. 7, pp. 85727-85745, 2019, doi: 10.1109/ACCESS.2019.2925010.

55. O nas. (2020, October 29). Retrieved October 9, 2022, from https://vouchforme.co/sl/o-nas/

56. Oderkirk, J. & Slawomirski, L. (2020, December). *Opportunities and Challenges of Blockchain Technologies in Health Care*. Retrieved October 9, 2022, from https://www.oecd.org/finance/Opportunities-and-Challenges-of-Blockchain-Technologies-in-Health-Care.pdf

57. Popovic, D., Avis, C., Byrne, M., Cheung, C., Donovan, M., Flynn, Y., Fothergill, C., Hosseinzadeh,Z., Lim, Z., & Shah, J. (2020). *Understanding blockchain for insurance use cases*. British Actuarial Journal, 25, E12. doi:10.1017/S1357321720000148

58. PricewaterhouseCoopers (PwC). (2017). *Blockchain, a catalyst for new approaches in insurance: Part 1*. Retrieved October 9, 2022, from https://www.pwc.com/gx/en/industries/financial-services/publications/blockchain-a-catalyst.html#:~:text=By%20removing%20intermediaries%20in%20a,difficult%20to%20define%20until%20now.

59. R3 (2020). *B3i Case study: Enabling and Accelerating Insurance and Reinsurance Industry Transformation with Distributed Ledger Technology*.

60. Raikwar, M., Mazumdar, S., Ruj, S., Gupta, S. S., Chattopadhyay, A., & Lam, K. Y. (2018, February). *A Blockchain Framework for Insurance Processes*. 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018, pp. 1-4, doi: 10.1109/NTMS.2018.8328731.

61. Salmon, J. (2017, September). *Blockchain/DLT in the Insurance sector*. Hogan Lovells.

62. Sandner, P. (2020, December 08). Will blockchain replace clearinghouses? A case of DVP post-trade settlement. Retrieved October 9, 2022, from https://www.forbes.com/sites/philippsandner/2020/12/02/will-blockchain-replace-clearinghouses-a-case-of-dvp-post-trade-settlement/?sh=3564ccf5408

63. Saxena, S. & Kumar, R. (2021). *The impact on supply and demand due to recent transformation in the insurance industry*. Materials Today: Proceedings, 56, 3402-3408. doi:10.1016/j.matpr.2021.10.337

64. Sayegh, K. (2018, October). *Blockchain Application in Insurance and Reinsurance*. Retrieved October 9, 2022, from https://www.researchgate.net/publication/327987901_Blockchain_Application_in_Insurance_and_Reinsurance

65. Shaker, M., Shams, F. & Fotohi, R. (2021*). Online rating system development using blockchain-based distributed ledger technology.* Retrieved October 9, 2022, from https://www.researchgate.net/publication/348426918_Online_rating_system_development_using_blockchain-based_distributed_ledger_technology

66. Sharma, T. (2020, March 26). 5 key challenges for blockchain adoption in 2020. Retrieved October 9, 2022, from https://www.blockchain-council.org/blockchain/5-key-challenges-for-blockchain-adoption-in-2020/

67. Sheth, A. and Subramanian, H. (2020). *Blockchain and contract theory: modeling smart contracts using insurance markets.* Managerial Finance, Vol. 46 No. 6, pp. 803-814. https://doi.org/10.1108/MF-10-2018-0510.

68. Sheth, H. & Dattani, J. (2019). *Overview of Blockchain Technology.* Asian Journal of Convergence in Technology, V(I), 1-3. Retrieved from https://asianssr.org/index.php/ajct/article/view/728

69. Singh, S. K., & Kumar, S. (2021). *Blockchain Technology: Introduction, Integration and Security Issues with IoT*. Retrieved October 9, 2022, from https://arxiv.org/ftp/arxiv/papers/2101/2101.10921.pdf

70. StartUs Insights (2019, January 18). *Blockchain Startups Disrupting The Insurance Industry*. Retrieved October 9, 2022, from https://www.startus-insights.com/innovators-guide/8-blockchain-startups-disrupting-the-insurance-industry/

71. Takashima, I. (2017, October 16). *Blockchain: The Ultimate Guide To The World Of Blockchain Technology, Bitcoin, Ethereum, Cryptocurrency, Smart Contracts.* Kindle Edition.

72. Takyar, A. (2022, September 26*). Proof of work vs proof of stake : An in-depth discussion*. Retrieved October 9, 2022, from https://www.leewayhertz.com/proof-of-work-vs-proof-of-stake/

73. Tapscott, D. & Tapscott, A. (2016). *Blockchain Revolution: How The Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin Random House, New York, NY.

74. Tarr, Julie-Anne (2018). *Distributed ledger technology, blockchain and insurance: Opportunities, risks and challenges*. Insurance Law Journal, 29(3), pp. 254-268.

75. Treiblmaier, H. & Beck, R. (2019). *Business Transformation through Blockchain (1st ed., Vol. I).* Palgrave Macmillan Cham. doi:https://doi.org/10.1007/978-3-319-98911-2.

76. Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). *Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends*. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(11), 2266-2277.

77. Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., ... & Kim, D. I. (2019). *A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks*. IEEE Access, 7, 22328-22370.

78. Wikipedia. (2022, October 03). Lemonade Inc. Retrieved October 9, 2022, from https://en.wikipedia.org/wiki/Lemonade,_Inc.

79. Wild, J., Arnold, M., & Stafford, P. (2015, November 01). *Technology: Banks seek the key to Blockchain.* Retrieved October 9, 2022, from https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64#axzz3qe4rV5dH

80. Williams, R. C. (2017, April). *Prospects for blockchain-based settlement frameworks as a resolution to the threat of de-risking to Caribbean financial systems*. Retrieved October 9, 2022, from https://www.researchgate.net/publication/316548562_Prospects_for_blockchain-based_settlement_frameworks_as_a_resolution_to_the_threat_of_de-risking_to_Caribbean_financial_systems

81. Writer, S. (2017, October 12). *Blockchain will do for re/insurance what the internet did for information: IBM interview*. Retrieved October 9, 2022, from https://www.reinsurancene.ws/blockchain-will-reinsurance-internet-information-ibm-interview/

82. Xu, M., Chen, X., & Kou, G. (2019). *A systematic review of blockchain*. Financial Innovation, 5(1), 1-14.

83. Yaga, D., Mell, P., Roby, N. & Scarfone, K. (2018, October). *Blockchain Technology Overview* (internal report). National Institute of Standards and Technology. NISTIR 8202, 1-57. doi:10.6028/nist.ir.8202

84. Yeoh, P. (2017). Regulatory issues in blockchain technology. Journal of Financial Regulation and Compliance, 25(2), 196-208. doi:10.1108/jfrc-08-2016-0068.

85. Yu, T., Wang, A., Tseng, L., & Tsao, W. (2021). *A Preliminary Study of the Impact of Blockchain Technology on the Application Level of Insurance Industry.* 2021 IEEE International Conference on Social Sciences and Intelligent Management (SSIM), 2021, pp. 1-5, doi: 10.1109/SSIM49526.2021.9555203.

APPENDICES

Appendix 1: Povzetek (Summary in the Slovene language)

Blockchain tehnologija je v zadnjih letih deležna velike pozornosti v osrednjem tisku. V zadnjem desetletju se je na področju blockchain tehnologije zgodil hiter razvoj (Fuchs, 2019). To je pritegnilo ogromno zanimanja tako s strani raziskovalnih skupnosti kot tudi industrije (Mingxiao, Xiaofeng, Zhe, Xiangwei & Qijun, 2017). Blockchain tehnologija je veliko več kot njegova prva povezava s kriptovaluto Bitcoin in pogosto se ta dva izraza enačita, kar je napačno. Blockchain tehnologija je nova vrsta podatkovne strukture, decentraliziran, nespremenljiv knjigovodski sistem za urejanje podatkov o transakcijah (Fuchs, 2019). Blockchain tehnologija ima številne potencialne namene, ki presegajo ozko področje digitalnih valut in kriptovalut (Svetovna banka, 2017). Ima potencial za preoblikovanje svetovne zavarovalniške industrije. Zavarovalništvo je bistveno pomembna institucija, zato je primerna tarča za razvoj v smislu zmanjšanja tveganja in kompleksnosti z vidika tehnologije. (Kim & Mehar, 2019). Potencialni primeri uporabe za zavarovalnice vključujejo inovacije zavarovalnih produktov in storitev za rast, povečanje učinkovitosti pri odkrivanju goljufij in določanju cen ter zmanjšanje upravljalnih stroškov. Poleg tega bi s tem lahko reševali nekatere glavne izzive, s katerimi se soočajo danes - na primer omejeno rast na zrelih trgih in pritiske za zmanjšanje stroškov (Lorenz et al., 2016). Blockchain tehnologija in pametne pogodbe bi lahko pripomogli tudi k avtomatizaciji regulativnega poročanja ter ga naredili učinkovitejšega in preglednejšega, izboljšali doslednost in kakovost podatkov ter regulatorjem omogočili dostop do podpisanih pogodb in informacij, ki jih vsebujejo v realnem času (regulativno spremljanje v realnem času). Vendar lahko sprejetje blockchain tehnologije povzroči tudi nova tveganja za zavarovalnice, nadzornike in potrošnike. Gre za novo in nastajajočo tehnologijo, ki se sooča z več izzivi, kot so kompleksnost tehnologije, varstvo podatkov in zasebnost, pravni status pametnih pogodb, kibernetsko tveganje, integracija z obstoječimi infrastrukturami ali medobratovalnost in standardizacija med različnimi blockchain tehnologijami (EIOPA, 2021). Namen tega magistrskega dela je raziskati potencialno uporabo veriženja blokov v zavarovalništvu ter pregledati možne primere uporabe in glavne ovire pri njegovi uporabi. V tem magistrskem delu bo razložena zgodovina blockchain tehnologije in ovrednoten trenutni status ter možnosti za napredek v zavarovalništvu v prihodnosti. To bo doseženo s poglobljenimi intervjuji s strokovnjaki iz zavarovalniške industrije. Struktura je razdeljena na tri glavna področja. Najprej je splošni uvod v blockchain tehnologijo, njene značilnosti, načela, ki stojijo za njo, in različne vrste porazdeljenih knjig ter uvod v pametne pogodbe. V naslednjem poglavju si bomo podrobneje ogledali, kako bi ta tehnologija lahko izboljšala zavarovalniško industrijo. Poleg glavnih področij uporabe, govorimo tudi o pobudi B3i in njenem vplivu na razvoj in sprejetje tehnologije veriženja blokov v zavarovalništvu. Ogledali si bomo pionirje v panogi, kdo so in kakšne vrste rešitev na podlagi veriženja blokov ponujajo v svojih poslovnih modelih. Nazadnje bomo razpravljali o vseh izzivih, s katerimi se sooča ta tehnologija, katere so glavne ovire in kako jih je mogoče premagati in rešiti pri prihodnjem razvoju te tehnologije. Zaključili bomo z raziskovalnim delom magistrske

naloge, s katerim želimo s poglobljenimi intervjuji s strokovnjaki iz panoge podrobneje obdelati vpliv blockchain tehnologije na zavarovalniško industrijo.

Appendix 2: In-dept interviews; Methodology and Q&A

Methodology

To determine the scope of the study and the preliminary interview questions, the thesis employs the literature review methodology. Academic web databases held the majority of the sources and work cited in the thesis (e.g., ProQuest Direct, Emerald, Science Direct, Sage). Papers are research papers created by industry leaders, consulting firms, and academic institutions. The in-depth interview is the primary qualitative research method used in this thesis. The rationale behind this decision is that qualitative research effectively conveys the views and opinions of insurance experts regarding the integration of blockchain and insurance. The interviewees chosen for the study are primarily insurance experts with blockchain expertise. These insurance professionals have extensive knowledge of how insurance companies implement policies and make decisions; in February 2022, qualitative research was carried out by inviting these professionals to participate in in-depth interviews. This master thesis would also conduct a parallel in-depth interview with Slovene experts with the research paper "A Preliminary Study of the Impact of Blockchain Technology on the Application Level of Insurance Industry" by Yu, Wang, Tseng, and Tsao (2021), which addresses the same topic using the same research methodology.

This thesis will show the true motivations for the study object and background data. Carefully explain the techniques and procedures of information gathering, moreover, it will genuinely illustrate the challenges inherent in the study field based on actual conditions. Its goal is to make future research easier and to identify the environmental and social contexts of the research objects. The questionnaire approach chosen in the in-depth interviews is undeniably credible, transferable, dependable, and confirmable.

In-depth Interviews

1. How would you describe Vouchforme / Adacta Fintech?

A: VouchForMe (VFM) is a startup company which is trying to disrupt the insurance business and bring it back to its roots, where the community was involved in sharing risk.

B: Adacta is a leading provider of core insurance platforms. With more than 30 years in the fintech business, we are both – seasoned professionals with more than 50 implemented projects across Europe, as well as a newcomer in the global market with our flagship product – Adinsure 3rd generation, which is based on the latest technology

steps. Our mission is simple: empower tomorrow's industry leaders to reach their full potential through technology.

2. As a VP of Business Development / As a CEO of Adacta Fintech, how do you view the impact of blockchain on the future of insurance industry digitalization? So far, how was the insurance industry impacted by these recent innovations?

A: Blockchain can be viewed as one of the technologies which drive the digitalization process in the insurance sector and beyond. It can help automatize some processes and make them bulletproof in a sense of potential fraud or human mistake. The insurance industry has and is adopting this innovation, but as insurance companies are very slow at implanting new stuff, the same holds here.

B: Blockchain has been present in Insurtech for more than 10 years; it is my feeling that the big announcements we were able to hear at the very introduction of blockchain in insurance have somehow missed out. Sure, there are young and prospective digital insurers based on the blockchain, but so far, they have failed to live up to expectations.

3. What is your opinion on the blockchain?

A: I'll give the analogy: since central banks will in a few years implement digital currencies on blockchain, this will splash out all the doubts about the implementation of this technology also in the insurance sector.

B: I believe that the true power of blockchain has been somehow overshadowed by the inflation of cryptocurrencies, as well as some failed ICOs, which, in consequence, gave a bad name to the technology itself. I still see a lot of potential in the blockchain, but fluctuation in the currency prices makes market leaders in the financial industry reluctant to jump aboard.

4. Do you think that the implementation of blockchain in the insurance industry is possible?

A: Yes. It's already happening.

B: Implementation is a very wide term. Lemonade was pivoting the effort to introduce blockchain in the industry, but their poor financial results and forecasts made others challenge the approach. The greatest benefit of blockchain, is the permanent keeping of records has far greater use for the authorities regulating the financial markets than for the final consumers themselves, therefore I believe that the greatest usage of the blockchain in insurance will prove to be in the regulatory area and not as much in the business area itself.

5. From your point of view, what are the main opportunities that arise from the use of this new technology in the insurance industry?

A: New products, less fraud and lower operating costs for the insurance company.

B: Answered in the previous question.

6. How would the use of blockchain change the business model of insurance companies? Could you make a comparison between the business model of platforms such as Vouchforme with traditional insurance business models?

A: The table below summarizes the key differences:

Table 1: Key differences

	Traditional	InsurTech	BlockChain
Transparency	Low	Medium	High
Operating cost	High	Low	Low
Flexibility	Low	High	Medium / High
User experience	Poor	High	High
Mobile / Internet	Low	Medium / High	High
Insurance prod.	Traditional	Traditional / Innovative	Innovative (smart contract + oracles)
Price	High	Medium / Low	Low + paying in crypto currencies

B: I don't think it can.

7. How does the use of Adacta's platform change the business model of its users?

B: Adacta aims to empower users to take ownership of their IT requirements, by providing them with low-code/no-code tools where they can introduce new products, processes, and regulations quickly and at low cost on their own. As an insurance platform vendor, we are aiming at providing our customers with the technology to ease their lives and make them more independent from guys like us. Hence, ease of use with a bunch of preconfigured insurance processes is the key driver behind our agenda from both perspectives – speed to market as well as cost-cutting.

8. How do you see the future of the insurance industry? Do you think that smart contracts are "the next big thing" for the insurance industry?

A: The insurance industry is evolving like any other industry. Blockchain (and smart contracts) is just one of many technologies that will impact our world.

B: You will see or hear people arguing that smart contracting will make all the difference in the world, but when you ask exactly how this will be a game-changer answers are somehow missing out. Litigating insurance contracts is expensive due to different interpretations of terms and clauses by the opposite sides, not because someone forgot to write something down or the contract was somehow lost. Sure, things might get speeded up, but it truly is not a game-changer. In the end – it's a bit too late now to consider

something „the next big thing “since the notion of smart contracting has been present for more than 10 years. It would already have happened if it was meant to be.

9. Are you familiar with the application of smart contracts in other industries? Do you believe that the same patterns could be used in the insurance industry? Can you give examples?

A: Yes, blockchain is used also in other industries like banking & payment, E-state, Online notary, energetic sector, IoT, Accounting, audit, compliance, RM, Distribution networks… One example could be tracking the origin of the food that we are buying at the local store…

B: I believe that banking is a more suitable ground for smart contracting than insurance. The main reason lies in some very complicated terms and conditions of the insurance contract, which, again, are subject to change and open for interpretation. I have seen (hold in my hands) 600 pages long insurance contract for one of the biggest transportation companies in the world and I promise you, no one is questioning if the contract was signed, but the sole nature of the „promise” within the contract.

10. Which aspect of the insurance business would be disrupted the most, and which will benefit the most from the use of blockchain?

A: In the beginning claims and payments can get all the heat, but eventually all the processes can be linked to this technology.

B: Insurance, as a notion, has been present since the stone age (people taking care of other people in times of need). Later on, in the Byzantine empire, people discovered that they could hedge their risks for a proper price and the insurance industry was born. Sure, a formal framework came a few millennia later on, but not much changed in essence – you pay a price for someone to pull your risk. Since then, people are using various instruments of insurance according to their needs and preferences. With the printing press (XV century) insurance became more widespread and slowly became one of the central parts of the world economy and every discovery since then just boosted the use of insurance. People were saying 30 years ago that the internet will „disrupt “ insurance as we know it, but that never happened. Insurers just find their way to use all the advantages of the latest technologies to improve in different areas, but in the end, they are still doing the same thing – taking a portion of your risk for a proper price.

11. How do you see Vouchforme evolving in the future as blockchain matures and gets more mainstream?

A: As a startup, VFM has offered different business proposals, some of them using blockchain. At the moment, we are still observing how the proposals will evolve. To be honest we are still very early into this technology.

12. How do you see Adacta keeping up with the future and the new challenges that arise with the use of new technologies such as blockchain?

B: Our RnD department is constantly experimenting with the latest technologies and concepts. We have been tackling blockchain some 8 or 9 years ago and since then we have shifted more toward AI and Machine Learning which we believe lies far greater benefit for our current and future customers.

13. What are the main obstacles to the implementation of new technologies in this industry?

A: Mainly people who are scared of new stuff. The fear comes out of not knowing the technology.

B: Insurance is a traditional craft, not very reluctant to be the first to jump aboard. The essence of the insurance industry is proper risk management and it is hard to believe that someone is managing your exposure properly if they are the first ones to test out the latest tech in practice. Nevertheless, insurers are investing enormous resources in understanding how they can leverage new technologies for their benefit, but as far as I can see, not too much has been implemented in the real life.

14. Do you think that the Slovene insurance industry is oriented towards new technologies, such as blockchain? Are they following the new developments in the industry worldwide?

A: Slovene ins industry is lagging behind the implementation of new technologies so at the moment I'm not aware of any Slovene insurance company doing anything in the blockchain field.

B: I don't see Slovenia as one pivoting the effort within the blockchain industry – although there have been some interesting start-ups in the past few years. The main reason is very tight regulation (on the EU level) which is reluctant to allow such „witchcraft" in regulated industries such as insurance. On the other hand, Slovenian insurers are trying to keep pace with the leading European insurers in terms of digitalization, customer relation and the usage of telematics in their everyday business.

15. What would be your advice for the leaders in the insurance industry?

A: Be open to new things and don't stop learning.

B: Advice is, of course, to keep track of the latest technological developments and to be focused on the speed to market and the usage of the enormous amounts of data they are sitting on top of. New risks are emerging every day and, so far, the insurance industry is failing to provide answers (proper products) to some of the most devastating risks for businesses (inability to attract talents, regulatory changes, failure to innovate) as well as for private persons (e-scooters, new viruses, emerging hobbies, etc).