DEGREE PROJECT IN COMPUTER ENGINEERING,
FIRST CYCLE, 15 CREDITS
STOCKHOLM, *SWEDEN 2017*

Blockchain, the future opportunity for trading progression?

Blockkedjan, framtiden för digitala överföringssystem?

TONY TRAN

MATS LEVIN

KTH ROYAL INSTITUTE OF TECHNOLOGY
SCHOOL OF TECHNOLOGY AND HEALTH

Blockchain, the future opportunity for trading progression?

Blockkedjan, framtiden för digitala överföringssystem?

TONY TRAN

MATS LEVIN

Bachelor in Computer Engineering
Date: June 13, 2017
Supervisor: Anders Lindström
Examiner: Ibrahim Orhan
TRITA-STH: 2017:37
KTH The School of Technology and Health

Abstract

The rapid expansion of computer technology have forced several business sectors to integrate with the continuous development of techniques in order to assist them in various tasks. Many fields have happily embraced the technology implementing it in numerous ways, however the development speed have proven difficult to keep up with. The insurance industry have struggled with ridding themselves of old and monolithic legacy systems with a haphazard construction. These systems are costly, cumbersome and often reliant on a “third party” centered structure creating such flaws as data leaks and monopolisation.

Blockchain is a distributed ledger operating over a peer-to-peer basis, with the intention to unshackle contemporary system from their dependence towards central authorities. Additionally, the peer-to-peer architecture introduced a new form of transparency which differs from contemporary solutions used in centralised systems, beyond the peer-to-peer architecture, the blockchain also incorporated consensus algorithms, allowing peers to verify one another to achieve consensus regarding the validity of each block. This resulted in a "trustless system" considering no single party in the community is dependent on the credibility of a central authority.

In order for the blockchain technology to be applicable on the market it must overcome obstacles such as privacy and the new EU data protection regulation “General protection data regulation”. However a vague definition of personal data have caused ambiguity which appears to be irreconcilable with the blockchain technology. Research have therefore shifted its focus to explore opportunities for the technology to collaborate with techniques from centralisation in order to overcome its obstacles.

Sammanfattning

Datorteknologins hastiga expansion har bidragit till att mängder av olika yrkessektorer tvingats integrera teknologin i sin dagliga verksamhet för att bidra med vissa uppgifter. Då teknologin i stor utsträckning har varit till nytta har många yrkesgrupper välkomnat den, dock har teknikens utvecklingshastighet visats vara mycket hög vilket medfört viss problematik. Försäkringsbranschen har visats ha problem med att hantera vidareutvecklingen av sina gamla monolitiska "legacy" system då de är både utdaterade och konstruerade på ett ostrukturerat sätt. Dessa gamla system är kostsamma, svårhanterliga och baseras ofta på en systemarkitektur centrerad kring "tredje parter" detta medför problem som dataläckor och monopolisation.

Blockkedjan är ett distribuerat journalsystem som struktureras med ett peer-to-peer nät som bas. Detta görs med förhoppningen att kunna frigöra existerande system från centrala autentiseringsparter. Dessutom har blockkedjan introducerat en ny sorts transparens som skiljer sig från de nuvarande centrala systemen. Blockkedjan inkluderar också consensus algoritmer som medför att alla deltagare kan verifiera varrandra och därmed nå ett uniformt beslut om blocks validitet. Dessa egenskaper resulterar i ett system som inte är beroende av att dess användare behöver lita på en centraliserad tredje part.

För att blockkedjan ska vara användbar och framgångsrik på en öppen marknad finns vissa funktionskrav som måste uppfyllas. Ett av de främsta av dessa är EU förordningen "General protection data regulation". Problem har uppstått då "General protection data regulation" innefattar vaga definitioner av "personlig data", dessutom är de existerande tolkningar av konceptet svår applicerade för blockkedje tekniker. Detta har bidragit till att utvecklingen av rena blockkedje lösningar har stagnerat och utvecklingen dirigerats om till forskning inom hybrid teknologier som inkluderar tekniker från centraliserade system.

Acknowledgement

We would like to give special thanks to the people who have assisted us during the research and work performed to complete this thesis. From KTH we would like to thank Anders Lindström who have acted as our mentor and Ibrahim Orhan who is our examiner. Additionally we would like to thank the people from Itello who have helped us with special recognition to Henrik Allert, Jacob Funck and Sofia Eriksson who have been great assistance whenever we have needed guidance. Finally a special thank you to Voone Laan and Mattias Andersson for taking time to help us deepen our understanding of international and Swedish laws.

Contents

Abbreviations & Glossary

Abbreviations

CoT Circle of Trust

DHT Distributed hash table

$GDPR$ General Data Protection Regulation

$IPFS$ Interplanetary file system

$P2P$ Peer-to-Peer

POW Proof-of-Work

ZKP Zero Knowledge Proof

Glossary

$ACID$ Atomicity,Consistency,Isolation,Durability

$BASE$ Basically,Available,Soft State,Eventual consistency

DAO Decentralised autonomous organisation

$divide\ and\ conquer$ An algorithm based on breaking down a problem into several sub-problems

$hash\ link$ A combined result of hashing the nonce and timestamp from the transaction

$hash\ value$ The result of a hash function

$immutable$ Data which cannot be altered

$linked\ list$ A linear collection of nodes pointing forward to the next node constituting in a structure

$nonce$ Random generated number only used once

$Ponzi\ scheme$ A fraudulent investment operation

$Quasi-identifier$ An identifier that requires additional data in order to identify any particular data

$SHA-256$ A hash function

$timestamp$ The time a particular transaction is requested

1. Introduction

Ayesha Khanna [1] states that financial institutions as well as insurance systems have in the past struggled to keep up with new regulations and the ever expanding financial market. This is commonly related to not being able to relinquish their dependency on legacy systems. Legacy systems have several issues such as their substantial maintenance cost. Another key aspects seldom present in legacy systems is the capability to facilitate fraud detections during transactions. Additionally legacy systems have had a tendency to rely heavily on "third parties" constituting a substantial security flaw as centralised units often represent a "single point of failure". Year 2008 started with the introduction of the cryptocurrency Bitcoin arriving in conjunction with a technology called Blockchain serving as its backbone. Blockchain have built excitement towards distributed systems by discarding centralisation and in doing so opening new opportunities for further development. This excitement has since the emergence of blockchain propagated over to different sectors such as insurance and health care.

The blockchain technology is a distributed communal Peer-to-Peer ledger that maintains a record of all transactions in the network and updates all participants accordingly. Through this communal structure any participant in the blockchain network can verify the integrity of transactions and thus relinquish the need for central authorities or "third parties" as they are commonly called. By making the system highly transparent the blockchain technology attempts to solve two common problems encountered in systems currently in use. Blockchain attempts to make data falsification as difficult as possible, this is achieved by having all transactions traceable as well as verifiable by any peer in the network. Additionally the "double spending problem" is also addressed, through usage of security utilities called hash functions and digital signatures, the blockchain attempts to make it impossible for a user to spend the same money twice.

1.1 Purpose

Due to the blockchain technology being in its infancy, uncertainties regarding how the technology handles regulated markets such as the insurance sector and scenarios like insurance trading has yet to be researched.

In order for the blockchain technology to have impact on the insurance industry it must satisfy requirements such as EU's General Data Protection Regulation(GDPR). Additionally to apply the technology in the insurance sector several requirements spanning from security to transparency must be satisfied, due to the insurance sector being under scrutiny of different government agencies. Additionally the new EU regulation GDPR regulates sensitive data, requiring a storage technology to be applied such that authorised parties have the opportunity to overview and audit transactions, while still preserving the integrity and confidentiality in their personal data. Lastly for the technology to be of interest it must be able to handle analogous scenarios but with differing laws and regulations such as an insurance trade between several parties versus a health record trade between different hospitals. Given the fact that differing laws and regulations could affect the outcome of how the blockchain technology is applied one must take different approaches in order to meet these requirements.

This thesis aims to answer the following questions:

- Is it possible to perform transactions between several companies using the blockchain?
- Which current blockchain architecture is most suited for these specified use cases?
    1. Transfer an insurance between multiple parties using the blockchain?
    2. Alter insurances for objects, persons e.g. change a car insurance from one car to another?
- Are there any regulations that would prevent blockchain from succeeding in the insurance industry?
- What are strengths and weaknesses of blockchain when regarding requirements facing contemporary systems?

This thesis will be useful for anyone who attempts to acquire general knowledge regarding blockchain architecture and its applications within the insurance industry. Additionally difficulties and circumstances forcing de-

velopers to take a different approaches when applying the blockchain will be outlined.

1.2 Scope

This study will research applications for the blockchain technology in the insurance sector. In order to limit the scope of this study it will only consider laws and regulations concerning the Swedish market. Additionally this study aims to observe insurance trading as a general purpose rather than delve into specific insurances such as life or house insurance. This study will also only touch on the subject of laws and regulations in order to observe whether or not they could create complications that would make a blockchain architecture unsuited for this type of problem. Lastly the study will not include an implementation to demonstrate the principle seeing as the technology will take the EU regulation GDPR into consideration, however since it has yet to be released it could therefore not be properly tested.

2. Theory and Background

This chapter presents background information required to review and comprehend this study.

2.1 Related works

The systems currently in use by the insurance industry are often old and monolithic having cores that have remained virtually unchanged since their creation. Additionally these systems have often been constructed in a rather haphazard way seeing as functionality has simply been stacked on an unstable core system as needs arose. This way of constructing systems have created large incoherent frameworks which have proven to be cumbersome for companies to manage according to Ayesha Khanna [1].

Due to the enforcement of rules and regulations constraining the industry, storage of personal data has also been shown to be a strenuous task. Seeing as the regulations regarding personal data are strict the requirements of secure storage have forced many companies to use in-house data-centers or other intricate solutions. This have led companies to build complicated "legacy systems" which are often accompanied by high maintenance costs. Due to dependencies on these systems companies are stuck in the quagmire of choosing whether or not to continue using and paying for current systems or to invest in new technology with unknown ramifications. Lastly Ayesha Khanna [1] also states that data transfers and transactions are often dealt with through a cumbersome manual process, increasing the possibility for occurrences of human error.

Hypothetically a blockchain-based system could be a possible solution to alleviate the workload of this cumbersome process. The technology offers a new approach to digital trading possessing differing capabilities than centralised solutions, seeing as digital trades are performed in a decentralised manner, hence involvement of central authorities could be relinquished. The blockchain technology incorporates new techniques to combat problems present in contemporary centralised solutions. By introducing con-

sensus algorithms between peers as well as creating receipts recording all transactions ever performed in the ledger, the blockchain technology manages to combat issues such as monopolisation and double-spending in a way legacy systems have failed to in the past. In regards to contemporary centralised solutions the blockchain technology have aimed to construct a "trustless system", shifting their focus away from security and into transparency using an innate trust achieved by the fact that any peer possess the ability to verify the validity of transactions. Hence, the blockchain cannot currently offer security and privacy to the same extent as centralised systems.

The blockchain has found a lot of success throughout the years and has ever since the release of Bitcoin been in an upwards-aiming trajectory. Bitcoin were however first to discover the potential of blockchain and found immense success using the technology. Ever since bitcoin's release in 2008 different sectors ranging from healthcare to finance have researched whether the idea of a blockchain architecture would be applicable in their fields.

Applications for the blockchain technology is currently a hitherto unexplored field. However, there are several fields that resembles the use cases in the purpose chapter.

2.1.1 Bitcoin

Bitcoin is a Peer-to-Peer(P2P) digital payment system constructed to deal with transactions between multiple parties without the inclusion of a trusted broker. Digital signatures and cryptography are amongst the technologies leading to the solution. When Bitcoin first introduced the blockchain technology there were two ideas that differentiated them from a regular distributed system. Bitcoin attempted to make each transaction transparent in order to complicate falsification. Satoshi Nakamoto [2] proposed a solution to the "double spending problem" using a P2P network in conjunction with consensus algorithms and a distributed timestamp server. This worked by timestamping and hashing each transaction into an ongoing chain of hashes called "Proof-of-Work". This means that a record or block cannot be manipulated from the outside without redoing this so called "Proof-of-Work".

As Bitcoin technology spread around the world many could personally experience the efficiency and ease of using a peer-to-peer system for money transferal however naturally flaws were also discovered. One of the larger

limitations of a digital currency is the lack of a governing party during trading and specifically trades performed across borders. Since there is no international governing agency, settling trading disputes between individuals on various sides of the globe can be problematic. Additionally settling occurrences of theft can also be shown to be troublesome for many similar reasons, simply put Bitcoin is hampered by its lack of a third party. Bluntly put Bitcoin has limited usage and lacks many controlling features such as smart contract creation, this is one of the reasons Bitcoin lacks functionality on more regulated markets such a insurance. To some extent the greatest success of Bitcoin could be said to be the way they exposed the world to their underlying technologies like blockchain.

2.1.2 Smart contracts

Vitalik Buterin et al [3] presented a new approach to the blockchain technology when he introduced the world to his blockchain stack called Ethereum. Ethereum introduced a new concept called “smart contracts” which is essentially is a piece of code or a set of rules that could be executed on the blockchain according to Jacob Stenum et al [4]. These contracts could be used to create almost any sort of agreement between various parties. Vitalik Buterin [3] state that Ethereum smart contract implementation is completely open and unencrypted, as such the privacy in the system is limited.

Another blockchain implementation that embraced the “smart contracts” introduced by Ethereum is called Hawk. Ahmed Kosba et al [5] present a solution that provides confidentiality in their contracts through different cryptographical methods. This in turn allows users to become more diverse and choose their preferred level of security. In order to achieve this Hawk had to implement their system using something called managers, making them stray slightly from the original “no third party” premise of the blockchain technology. Finally the architecture of R3’s Corda also embraced the idea of smart contracts and distributed ledgers. Unlike other architectures such as Ethereum, Corda was not built as a general purpose model instead Corda was built with the explicit purpose of maintaining a shared ledger and enforce agreements among registered institutions within the financial sector.

The concept of "smart contracts" was introduced by Ethereum as a new approach to deal with negotiations; a smart contract is essentially an agree-

ment between several parties. Smart contracts were able to expand possible use cases for the blockchain and in doing so they were able to pique the interests of different sectors one of them being health care. Positive attributes can be derived from smart contracts but in conjunction with its strengths come some weaknesses. Due to smart contracts being a piece of code which is executed by the blockchain there exists possibilities for security breaches when handled incorrectly. Due to immutability in blockchain architectures bugs in smart contracts would remain forever since it cannot be altered. The Ethereum blockchain was previously vulnerable due to a bug in a smart contract, which was exploited this particular attack is according to Nicola Atzei [6] referred to as "the DAO attack". Due to containment lying in the Ethereum community's hands consensus had to be achieved whether or not a so called rollback or "hard-fork" as it is called should be made, or if the community should do nothing and allow the attacker to keep his loot. In the end the community decided upon a "hard-fork" because consensus algorithms only requires a majority and not all participants, leading to the part of the community which did not consent to a "hard-fork" losing confidence in the technology.

2.1.3 Health care

The blockchain architecture quickly emerged and has piqued the interest of the medical sector according to Ariel Ekblaw et al [7]. Different attempts to find several use cases for the blockchain technology is currently being researched. Laure A. Linn and Martha B.Koo [8] present a paper containing different use cases for blockchains in Health Care which addresses the subject of taking other approaches with the blockchain technology such as applying it as an "access control mechanism" towards health records, allowing the blockchain to control how peers access data stored on the blockchain. Thomas Hardjono et al [9] present additional studies which evaluates the possibility to transmit health records regarding certain individuals while still preserving the integrity and security of their personal data. Furthermore Thomas Hardjono et al [9] also evaluate whether the blockchain technology would be applicable to prevent personal data from being leaked to other parties. An example would be "algorithm requesting" which works by requesting functionality from the chain to be performed on an individual's data without them being required to send the data. A system structured this way enhances users ability to maintain control over their own personal data.

2.2 Laws

The insurance governing law in Sweden fall under two different acts called “the insurance business act” and “the insurance contracts act” or "försäkringsrörelselagen" and "försäkringsavtalslagen"(FAL) as they are called in Swedish. These two acts cover the laws and regulations pertaining to swedish inhabitants ability to obtain insurance coverage, payments and contract terminations. Lastly there is the “insurance broking act” which constitutes requirements which brokers must comply with and regulates how operations are being licensed according to Riksbanken [10].

2.2.1 Insurance business and contracts act

The insurance contracts and business acts are two regulations within Swedish law covering most rules regarding the insurance business. The business act covers regulations regarding insurance institutions as well as their creation and is as such of modest importance in regards to this paper [11].

The insurance contracts act stipulates regulations regarding the creation of insurance contracts and the necessary procedures required by both parties entering into the contract agreement. Seeing as this paper will regard transactions between insurance parties, and these may very well include the recreation of insurance contracts, the laws contained in the contracts act could be of some importance. A possible example of a transaction where the insurance contract act could come into play would be the transferral of a life insurance. If the new insurance agent desires access to the health records of an applying party, permission from said party is required for the agency to request said records from the health sector. This requirement for the insurant to grant access to the insurer is stipulated in the first paragraph of chapter seven in the insurance contracts act [12]. This would mean that an insurer would be required by law to obtain permission from a customer to review their health data. In the case of a transaction of an insurance, the receiving company would need to obtain permission at the start of a transaction to guarantee that the transaction is finished within the one day timeframe as stated in chapter three paragraph two [12].

2.2.2 General data protection regulation

In 2016 it was confirmed that all EU citizens will be protected by a regulation called “General Data Protection Regulation”(GDPR), which will replace the current “Data Protection Directive”. From 25 May 2018 organisations are obligated to be GDPR compliant, this in turn could affect applications for the blockchain technology.

2.2.2.1 GDPR compliance

The EU regulation GDPR puts pressure on different organisations to become compliant to the new regulations. GDPR is essentially a stricter version of the current “Data Protection Directive” or “Personuppgiftslagen”(PUL) that currently exists in Sweden.

The new regulation GDPR introduced by the EU [13] strives to support individuals in their pursuit to keep personal data private. A definition of personal data from the currently active regulation “Data protection directive” [14] is that “personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address”. The definition of personal data in the current directive is rather vague, considering the scale of data which is incorporated in the classification of personal data. GDPR being an extension of the currently active directive seems to continue the trend of ambiguous definitions of personal data. Amongst GDPR’s statements is that "The processing of personal data should be designed to serve mankind", where the definition of personal data could be anything spanning from IP-addresses and radio frequencies to DNA [13].

Further GDPR states that any individual should maintain the rights to access their personal data as well as find out how, where and for what purpose their personal data is being processed. An individual should also have the “rights to be forgotten” meaning their data must be removable. Additionally data should also be portable.

For anyone already familiar with the blockchain architecture it might be evident that the technology requires something more in order to achieve GDPR compliance. Vuk Kadenic [15] states an analogous problem for the Hadoop File System (HDFS) since a blockchain consists of immutable data

the issue of resolving "Right for erasure" still remains and achieving GDPR compliance becomes a more difficult task.

2.3 Blockchain techniques

The blockchain technology has caused a lot of commotion in the world especially in the finance sector, due to the rapid growth of the cryptocurrency bitcoin and its usage of the technology. Blockchain is a distributed ledger system with the additional ability to read and validate transactions embedded into the system.

Blockchain has taken a new approach towards traditional distributed database systems by shifting to peer-to-peer(P2P) interaction between different nodes in a system as stated by Nikola Bozic et al [16]. Unlike a traditional distributed system the blockchain was built using a different mindset and to meet a different set of requirements than one might find in a traditional database system.

An easy way to understand the structure of a blockchain is to think of the analogous data structure called a linked list. Each block contains some data such as a timestamp, a nonce and a record of transactions. Additionally each block also carries a hash link from its predecessor, which constitutes the chain part of the blockchain.

According to Nikola Bozic et al [16] blockchain strives to satisfy the following requirements

1. Guarantee authenticity of transactions in order to prevent problems such as double spending.
2. Transparent transactions i.e. each transaction should ensure traceability in order to make falsification as difficult as possible.
3. Maintain the chain's integrity from attacks etc, without the inclusion of a central authority.

When talking about different database management systems the terms ACID or BASE are commonly used. Both ACID and BASE systems are able to provide transactions. However traditional database systems enforce the fact that users have to trust something that from the outside might look like a "black box". This is due to the fact that clients can seldom control or

even observe the execution of their transactions. So instead users trust that their bank or other system follows a certain set of rules.

Blockchain is said to be an alternative to ACID and BASE that address this supposed trust issue and propose a system that allows transactions to execute independently without a central party, i.e the transactions become "trustless". A transaction that executes on the blockchain is neither ACID or BASE however blockchain introduced a new term called SALT [17].

There are two different perspectives to the SALT alternative, namely a transaction-based and a system-based perspective. According to Stefan Tai et al [17] "SALT" from a transactional perspective satisfies the following properties.

Sequential: In a blockchain all transactions are processed sequentially i.e there cannot be any parallel execution of transactions in the SALT model. It is through this that the blockchain incorporates the isolation property retrieved from ACID transactions.

Agreed: Transactions are accepted and validated as soon as a majority of the network can attest to their validity. This means that the entire network has to reach some form of consensus rather than in traditional databases where there is some form of central authority that validates each transaction.

Ledgered: Whenever a transaction has reached the state “agreed-on” they are added to an “append only” transaction ledger where they cannot get revoked, i.e there are no state changes that can be altered. This ledgered property of blockchain is however slightly weaker than the durability property that exists in ACID, due to the “majority agreed-on” process.

Tamper-Resistant: Tamper-Resistance in the blockchain has two different dimensions to it. Tamper-resistance is commonly related to the fact that a transaction should not be able to be manipulated or get censored, whereas the two different dimensions refers to the fact that a transaction can be pending or “agreed-on”.

2.3.1 Permissioned and permissionless ledgers

According to Adam Albertsson and Rickard Wendeberg [18] blockchain ledgers can be divided into two separate categories namely permissioned and permissionless.

A permissioned ledger's validation process is performed by a selected group of participants which could be government auditors or a group of financial institutions. A permissioned ledger constitutes a structure that could be adopted in the near future for different organisations. The main difference between permissioned and permissionless is that each participant in the network has to be identified when applying a permissioned ledger.

A permissionless blockchain strives to create anonymous transactions where the validation process operates on a decentralised level through any participant in the network. Considering financial institutions are regulated a permissioned ledger might be more suited, due to institutions being able to maintain control of the blockchain themselves.

2.3.2 Mining

Aggelos Kiayias et al [19] explains the mining process in the following way. Mining is the process in which a block gets added to the blockchain. Miners are required to solve a difficult cryptographic puzzle in order to include a new transaction to the block. In order to create some incentive to mining, Bitcoin yields a corresponding reward whenever a block is added to the chain. When solving this cryptographic puzzle miners are challenged to find a so called nonce value. David Yermack [20] describes the nonce value as a one time random generated number with the additional property that when concatenated with the additional data from a block it will generate a hash value with a specific number of leading zeroes.

In order for pending transactions to work, blockchain applies a digital signature that only the creator of the transaction is able to generate. Furthermore there should be no other user in the entire system that are privileged to alter or block pending transactions. Also the chain is built in such a way that alteration to an agreed-on transaction would invalidate the integrity of the entire chain.

2.3.3 Hash functions

Bitcoin applies the hash function's property of "one-wayness" as a key functionality in their Proof-of-Work, which will be discussed later. Furthermore hash functions are a key element in constructing the foundation for Merkle Trees. Hash functions are functions that are able to receive data of

arbitrary length and produce an output of a predetermined length depending on algorithm. This output value is often called a hash value, which is always the same for equivalent inputs. Pedro Franco [21] states that a good hash function should be able to have a proportional distribution of input to hash values, such that there is a one-to-one relationship between them. According to Pedro Franco [21] there are some additional requirements that are common for hash functions to satisfy.

Trapdoor/One-wayness: Given a specific hash value it must be computationally infeasible to retrieve the input value from the hash value.

Weak collision resistance: The likelihood of several input values that produces the same hash value should be computationally infeasible.

Strong collision resistance: The likelihood of having exact two input values producing the same hash value should be computationally infeasible.

2.3.4 Merkle trees

A merkle tree is a binary tree constructed by using "secret leaf tokens" or hash values as they are commonly called. Each parent node is represented as the concatenation between its left and right child which is then passed through a hash function. Eventually the hash of the entire tree's root node is calculated, which is called a root hash or a Merkle root [21].

Pedro Franco [21] states that one of the biggest advantages of Merkle trees is the verification of transactions. A node that wishes to verify that a transaction belongs to a block on the blockchain could perform this operation in a logarithmic fashion. This is due to the fact that the node only has to compute all the hashes from the leaf and upwards towards the root branch rather than computing the entire chain.

Bitcoin embraced the merkle tree structure through a method called the Simplified Payment Verification (SPV). According to Pedro Franco [21] Bitcoin possess a simpler and more effective solution to verify that a transaction belongs in a block. By applying a so-called block header assembled through the merkle root, the nonce included by the miner itself as well as the hash of the previous block. Each SPV client was able to maintain copies of block headers from the longest proof-of-work chain, which could be retrieved through querying the network until the SPV client is

convinced that it possesses the longest chain. When a SPV client then attempts to verify that a certain transaction belonged in the block they could download a specific branch in the merkle tree containing the connection between a particular transaction to their respective block header called a "Merkle Branch".

According to Satoshi Nakamoto [2] nodes will always resolve conflicting branches (forks) by using the longest chain possible as if it were the most legitimate one. This means a node validates transactions through its existence within a block that belongs to the longest possible chain. This type of validity check is referred to as the block height validity check. However, SPV clients validates transactions though the number of blocks that has been mined on the block that contains the transaction, and is referred to as the block depth validity check.

2.3.5 Security techniques for the blockchain

The requirement to maintain security in messages across the network has been an issue for a long time. Cryptography is a technique that not only satisfies this requirement, it also offers additional properties beyond encrypting data, seeing as it could also be applied for authentication, digital signatures as well as integrity control as stated by Kapoor et al [22].

2.3.5.1 Zero knowledge proof

The zero knowledge proof system is a way for one party in a transaction to convince another party that they posses certain information without revealing any meta-data regarding the information. Zero knowledge proofs(ZKP) was according to Sultan and Clifford [23] originally used as a way for parties in an exchange to prove their identities to each other without sharing information that could be used to harm either party. The basis of ZKP lies in one party being in possession of a secret wishing to prove to another party that they possess this secret without actually revealing the secret or any information regarding it. A trivial walkthrough of ZKP could be explained if a communication between two parties is imagined. Party A knows a secret and intends to convince party B of this. Party B will then proceed to ask party A a series of yes or no questions which only someone who possesses the secret could answer. The actual amount of times the questions are asked varies but given enough times the likelihood of party

A convincing party B that it is not guessing the secret, but actually possesses it will increase. When party B is convinced party A is in possession of the secret the proof has been concluded.

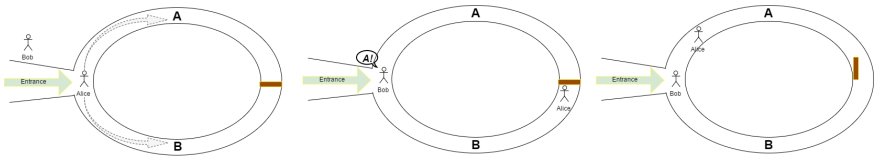

Figure 2.1: An illustration of Alibabas' cave example.

2.3.5.2 Digital signatures

Pedro Franco [21] explains digital signatures as an application of asymmetric cryptography whose goal is to achieve an insurance factor similar to an handwritten signature. Meaning a digital signature ensures that a message was generated by the signer and has not been tampered with. Additionally a digital signature enforces non-repudiation so that a signer shall never be granted the ability to deny a signature.

2.4 Implementations of blockchain-inspired architectures

This section introduces implementations and characteristics from different blockchain-inspired architectures.

2.4.1 Bitcoin

Satoshi Nakamoto introduced Bitcoin in 2008 and serving as its backbone was the technology Blockchain, innovating how distributed systems are thought about. The idea is to construct a system in which the community is able to join forces in order to construct consensus alongside algorithms such as "Proof-of-Work". By applying these techniques Bitcoin were able to remove the presence of central authorities common in contemporary

systems. This in turn removes opportunities for breaches of security arriving in conjunction with trust. Satoshi Nakamoto [2] achieved this through methods such as digital signatures, cryptography etc. with the main purpose of eliminating brokers within the system.

> "I think there were a lot more people interested in the 90s, but after more than a decade of failed Trusted Third Party based systems, they see it as a lost cause. I hope they can make the distinction that this is the first time I know of that we're trying a non-trust-based system." - Satoshi Nakamoto 2009, Pedro Franco [21] Understanding Bitcoin: Cryptography, engineering and economics

Bitcoin applied a technique called Proof-of-Work, which is a technique that applies timestamping and hashing transactions into an ongoing chain. This in turn means that in order for a block to be manipulated from the outside one must perform this Proof-of-Work again.

2.4.1.1 Proof of work

Bitcoin has implemented a distributed timestamp server built on a peer-to-peer basis, which applies a proof-of-work system similar to Adam Back's Hashcash [2, 21]. Bitcoin used the "proof-of-work consensus" as a way for someone to prove that a block required a certain amount of work to be mined. Proof-of-Work involves computing a value that when hashed with an algorithm, commonly SHA-256, results in a hash value beginning with a certain number of zero bits. Satoshi Nakamoto [2] claims that the average work a node has to perform is exponentially related to the number of zero bits required and is verifiable by a single hash. An example of this would be a simple coin toss, the result of finding x number of 0's followed by each other has the same probability as finding a sequence that contains x number of only heads or tails.

2.4.1.2 Attack towards Bitcoin

One way to attack the entire Bitcoin system is the scenario where an attacker attempts to build an alternate chain faster than the honest chain. However even with an alternate chain the attacks that could be performed would not be as crucial as one might think. Due to the fact that honest nodes would not accept an invalid transaction as a payment, nor would

they accept a block that contains an invalid transaction. What an attacker could attempt to do is to change their own transaction history in order to reclaim coins spent in earlier transactions.

The race between an honest chain and an attackers chain could be viewed as a Binomial Random Walk according to Satoshi Nakamoto [2]. The entire problem could be observed as a catch up game where every time the honest chain succeed in validating a block to the chain the gap between the honest and the attacking chain gets extended by +1 and for each block that gets added to the attackers chain the gap gets decreased by -1. This problem that Satoshi Nakamoto explained is analogous to the Gambler's Ruin Problem, which essentially entails calculating the probability of an attacker managing to catch up to the honest chain from a certain deficit.

Suppose that a gambler with unlimited credit begins at a deficit and plays a certain number of trials, potentially an infinite number, with the goal of trying to break even. It is now possible to calculate the probability that the gambler ever manages to break even, or in the case of blockchain the attacker ever catches up.

2.4.2 Ethereum

Ethereum is a blockchain architecture which stores so called smart contracts on the chain as information. Smart contracts works like a piece of code implemented onto a generic blockchain making it possible for users to trade not only information but to execute functions between parties, this according to Stenum et al [4]. Etherium works similarly to a decentralized computer or server if you will, making it possible to put programs on to the blockchain and use them to execute functions, these functions can be anything from voting systems to financial transactions. Ethereum is according to Vitalik et al [3] implemented with its own Turing-complete programming language which is used to write smart contracts. Ethereum consists of two currencies one of them being gas which a miner or user consumes for each execution step, this idea of a gas is to limit infinite loops, due to the fact that the miner/user would eventually run out of gas. Gas is also applied in the calculation of their other currency called Ether which Etherium applies as a in-house currency which is consumed as payment when transactions are executed.

Ethereum smart contracts are as mentioned code written onto a generic blockchain using the Turing-complete programing language implemented

into the Ethereum virtual machine as stated by Vitalik et al [3]. Etherium consists of so called accounts similar to objects in any object oriented language, however Ethereum have chosen to call these objects "accounts". An account can be identified by its unique 20 byte address. Accounts contains four fields, a nonce to ensure that a transaction is only made once, ether balance, contract code and storage. A account does however not have to contain any code seeing as there are two types of accounts in Ethereum, one is called contract account and the other is called externally owned account. A contracts account is as it sounds the accounts containing code or contracts if you wish, while the externally owned accounts are used to interact with the contract accounts according to Vitalik et al [3]. External and contract accounts could be thought of as a client-server-architecture where the externally owned accounts act as clients that communicate with contract accounts that possess the desired functionality expected from a server.

2.4.2.1 Attacks toward Ethereum

Nicola Atzei et al [6] presents a paper of different attacks that could be performed towards the Ethereum blockchain architecture. Some of the attacks mentioned in the paper are modelled as if they were games, one of these being the GovernMental. GovernMental is a kind of Ponzi scheme with a game-like structure, in order to join the scheme participants are obligated to insert a certain amount of ether to the contract. The last participant to join receives all ether in the contract if no participants were to join the scheme during the 12 hours after the last investment.

Furthermore Nicola Atzeri et al [6] presents three slightly different but similar versions of this particular attack.

Attack#1: The first version aims to exploit vulnerabilities within "stack size limits", this version is executed by the contract owner. The owner's purpose is to avoid the final transaction of the fee to the winner, leaving the ether in the contract redeemable by the owner themself at any point.

Attack#2: In this scenario, the attacker is a supposed miner impersonating a player. Being a miner allows for the opportunity to dictate transactions, and the miner could therefore choose to discard all transactions that are directed to GovernMental except for the miners themselves. Therefore the miner would become the last "player" in the round and

could claim its reward.

Attack#3: In this scenario the attacker remains a miner impersonating a player. However in this scenario the miner attempts to join the scheme, and still remain the last player. But rather than discarding current transactions the attacker attempts to tamper with the "block timestamps". If the attacker manages to publish the new block using a delayed timestamp the attacker would be the last player in the round and could claim its reward.

2.4.3 Hawk

The hawk framework is built on top of a blockchain and gives users the possibility to write decentralized smart contracts while keeping information private from others in the blockchain structure.

To allow privacy while using a blockchain architecture Hawk has implemented encryption at the compiling stage of contract creation, using zero knowledge proofs Hawk is according to Ahmed et al [5] able to maintain privacy through encryption. When a contract has been written it will be compiled into an encrypted protocol consisting of two parts, one of the parts will be a public one available to everyone and the second one will be the private part encrypted and stored on the blockchain. The private part contains functionality or rules required to execute the contract when all necessary data has been assembled. To allow data to be sent to the private part of a contract a middleman system called a manager has been introduced. The manager is a so called minimally trusted middleman and works by receiving data from the parties involved in a contract, when the data have been received the manager will send the data to the blockchain for contract execution. The term minimally trusted does according to Ahmed et al [5] mean that the manager has no opportunity to actually influence the contract execution, instead it works much like a relay and fact checker by simply receiving the required data and relaying it to the blockchain. Only when the data is sent and a transaction of some kind has taken place will the manager be able to view any data since it will have access to the encrypted messages sent to the blockchain. For this reason the manager is called minimally trusted; the only data it can actually see is data already used in a transaction.

2.4.4 Corda

R3's Corda is a distributed ledger technology with the intention to construct a system where financial agreements could be managed in a "trustless" fashion. Corda shares some similarities with the blockchain architecture however Mike Hearn [24] states that Corda is not a blockchain although they share several similarities. One of these similarities is that Corda is also a distributed ledger which operates on a Peer-to-Peer basis using several consensus algorithms. The main difference distinguishing Corda from a blockchain architecture is that transactions are not timestamped and aligned into blocks in order to resolve transaction races. Instead Corda resolve a transaction race through pluggable notaries.

According to Richard Gendal Brown et al [25] Corda also attempts to enforce privacy in the sense that they attempt to restrict data access to only the privileged participants that are entitled to it, whereas in most blockchain architecture transactions are open for anyone to validate.

3. Method

The study was conducted in order to gain insight into different blockchain architectures and choose an implementation that is capable of satisfying the requirements of previously stated use cases retaining to the insurance sector. Additionally information gathering regarding complications like GDPR and the blockchain's capability to cope with them is required.

Seeing as this paper would revolve around a hitherto unexplored application of the blockchain technology and as such had to consider several factors spanning from laws to architectures a literature study was chosen as the approach to information gathering. Naturally other approaches were considered however none were as comprehensive as a literature study and the possible unique advantages other approaches could offer were negligible. The information gathering consisted of perusing several related works and condensing the useful information into this paper.

Considering possible applications for the technology would reside within a regulated market constrained by rules which have yet to be released, an implementation would be flawed seeing as compliance could not be properly tested. As regulations have yet to be released this paper will result in a few hypothetical models prepared to face future constraints.

To validate the gathered information interviews with experienced personnel working in the field will also be conducted, the questions asked during these interviews can be read in the appendix chapter. The interviews were conducted because experienced individuals insights was considered more valuable than an implementation whose regulatory compliance is untestable. Through the interview insights into the respective fields could be gathered and condensed into information quintessential to evaluating the proposed models and concluding if they surmount contemporary systems. The interviews were conducted with a few key individuals possessing knowledge within fields useful for evaluation and information gather regarding the possible use of the models proposed in this paper. The questions were mostly focused around laws and especially privacy regulations in regards to the blockchain, additional follow up questions were conducted to gain insight in the models capability to face the challenge of

achieving compliance. To gather information regarding legal issues the models may face during implementation, interviews with a lawyer [32] knowledgeable regarding GDPR and a product owner [33] in the insurance tech business was performed. To further evaluate the models an interview with senior developers and head of research and development [34,35] was conducted.

The interviews were divided into to pre and post-interviews where the pre-interviews mostly revolved around defining the different use-cases for the thesis purpose as well as gaining some insights into general knowledge regarding blockchain. Different types of requirements a system within the insurance industry has such as GDPR was also discussed.

The post-interviews were mainly focused on privacy aspects revolving GDPR in regards to blockchain-based architectures. The questions regarded GDPR and the different requirements a model must fulfil in order to achieve compliance, as a follow up the questions also gauged how compliant the proposed models in the result chapter were.

4. Result

This chapter will present the results reached in the project, this will include summaries of information from interviews as well as hypothesised models solving the problem statement of the paper.

4.1 Result from interviews

This section will present information gathered through a series of interviews. Seeing as both pre and post interviews were conducted the results of these will be presented at different points in the paper. The results presented in this chapter will be information gathered during the pre-interviews while the post-interviews reflections are mostly in the discussion chapter.

4.1.1 Transactions

The systems currently used by the insurance industry for transactions of data are heavily reliant on a process consisting mostly of manual communication between the parties in a transaction. Seeing as companies use a multitude of old legacy systems, the transferal of data is often complicated because of varying file systems and data formats.

To properly explain a transaction what follows will be a step-by-step walkthrough of a simple hypothetical insurance transferral as desired by use case one in the purpose chapter. First company A receives the command to transfer an insurance, at this point the insurance data such as insurance-type and owner is reviewed and company B is contacted. When company B have been made aware of the transferal, they demand the required data for the creation of an insurance from company A. When company A has sent the data a new insurance is created by company B at which point company A is informed and removes the insurance in their possession. All of

this contact is mostly managed by employees through a manual process consisting of mailing and faxing data.

The second use case mentioned in the purpose chapter relates to updating the data contained in a contract. Currently this process is much like transactions a rather manual task usually performed by employees at an insurance company, following is a simple step-by-step explanation. When a customer desires to update an insurance contract they send information regarding their contract and customer data together with an update request to the insurance company. At the point when the company receives the request containing the information a validation process will be performed, this will include checking the customer data to be correct. If the validation is successful the company will update the data and and send a confirmation to the customer that the update have been performed.

4.1.2 Laws

Problems with the blockchain technology in relation to the new regulation GDPR has throughout this paper been outlined, however by evaluating the ranking in which different regulations applies it is stated that GDPR should be used when there are no legal obligations to store or process personal data. For example in Sweden there are laws regarding payment services [26] stating that transaction data is obligated to be stored for a certain period of time. In a scenario like this GDPR would apply after the time has expired.

An important factor to consider when interpreting laws is how ambiguous they can be regarding interpretations of phrases and content. An example important for this study is the phrase personal data, this phrase is defined as any data that could be used to identify a certain individual, however what that entails exactly is quite undefined. According to GDPR [13] identifiers could include everything from an ip-address to radio frequencies, this causes confusion on exactly what should be categorised as personal data. One consideration highly important for users of the proposed hybrid models mentioned later in this chapter is if key-identifiers in databases is considered personal data. So far it is not known exactly how key identifiers will be handled under GDPR and as such it is still unknown if they will be considered personal data or not.

4.2 Blockchain models

During the progression of the study a few possible alternatives for implementations of the blockchain technology have been researched. Throughout this chapter several possible ways of implementing the blockchain into a system architecture will be presented. Seeing as these models share their dependency on a few other technologies these will first be presented.

In order for the models to be viable on the market these characteristics are required to be combined in a new way. Currently blockchain is not competent enough to deal with privacy, additional research has therefore been conducted to grasp whether or not privacy could be achieved by taking another approach when applying the technology.

Public blockchains are currently not able to provide any level of privacy considering the blockchain is publicly open for anyone to participate in.

The natural architecture of a permissioned ledgers appears to be more suited for negotiation protocols. Considering, permissioned ledgers are constructed through a communal group of known parties with an innate trust. A negotiation protocol could be constructed such that peers are able to negotiate with each other without the inclusion of a third party.

4.2.1 Strengths and weaknesses with the blockchain technology

This section will introduce some abilities of the blockchain that could be treated as a strength or a weakness dependent on the situational use case.

When applying blockchain outside the realm of cryptocurrencies new incentives might be required in order to reward peers for their contribution while punishing malicious behaviour. An idea proposed by Guy Ziskind et al [27, 28] based on Ethereum's model but with an additional security deposit included to allow punishment of malicious behaviour. Each peer intending to participate in the network would be obligated to deposit a certain amount of bitcoins to a contract. If malicious behaviour were to be detected that peer's deposit would be split among the honest peers. Xiwei Xu et al [29] proposes an incentive which is not based on currencies where organisations could join forces in a permissioned ledger and exchange reputations or reviews. Seeing as it constitutes opportunities for companies to

market themselves it could yield an incentive for organisations to cooperate with each other despite being each other's opposition.

Considering a pure blockchain implementation requires a network of miners to collaborate and perform an immense task to maintain the system one evident weakness is the speed at which transactions could be performed. As such a blockchain-based system cannot even remotely compare to the performance achieved in centralised systems. Seeing as blockchain-based systems allows any participant to verify both integrity and correctness of each transaction, each peer must also possess the required data to be verified hence all data must also be replicated to each peer constituting a substantial amount of network traffic. To demonstrate the blockchains lack of performance a comparison with VISA have been made. VISA are able to process an average of 2000 transactions per second whereas Ethereum and Bitcoin processes on average 3-20 transactions per second which is a significant difference that could be diminished by the addition of an off-chain network and faster transaction validations according to Xiwei Xu et al [29]. Beyond that the strength in blockchain does not lie in terms of performance, instead it lies in transactions and more specifically how transactions are carried out as well as the introduction of tamper-proofed logs and immutable data.

Immutable data has both positives and negatives the strength being that once a transaction has been executed it will be stored in the ledger for all eternity without possibility for alteration. A transaction could therefore be used to trace back to their origin in cases of fraud or other malicious behaviour. However the downside with immutable data is that personal related data would also be stored on the ledger without the possibility for alteration and therefore achieving compliance becomes more of a daunting task.

4.2.2 Blockchain in a trust circle

During the construction of a system architecture there are a myriad of possible ways a blockchain structure could be implemented. One of these structures is called "Circle of trust" (CoT) and will be explained in this chapter. The "Circle of trust"-architecture is based around the usage of the permissioned blockchain concept and uses a host of trusted parties as members and miners of an internal blockchain.

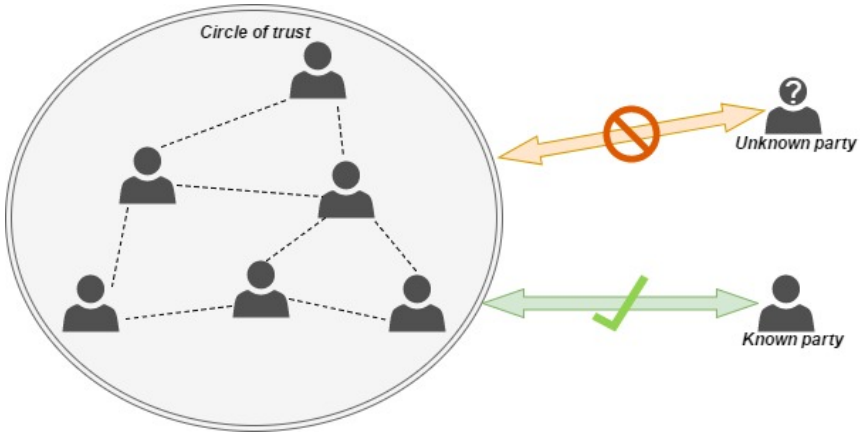

Figure 4.1: An illustration of a "Circle of Trust".

As mentioned earlier and also shown in figure 4.1 a “Circle of Trust” only invites known and trusted parties and as such it only consists of cooperating entities. By only consisting of known parties collaborating towards a common goal the CoT is able to force cooperation between parties and to some extent create trust, this most likely being the greatest strength of the model. Through usage of CoT multiple parties can share data through a trusted system allowing companies usually in competition to cooperate and trade data. An additional possible benefit of the CoT is the transparency inherently contained in systems using the blockchain technology; this strength can be especially useful if transactions between parties in the CoT requires some kind of overview from a third entity like a government agency. Through inviting the agency into the CoT they are given the option to view and evaluate transactions performed within the circle.

Naturally the CoT model also possesses certain weaknesses, the inherent weaknesses of the blockchain architecture is still present when using the CoT model although the usage of pseudonyms has been removed allowing parties to know of each other. Additionally the CoT model also has a problem mentioned earlier which is the incentive to mine. Seeing as there are no obvious large benefits to mine appart from the blockchains continued construction the mining incentive compared to a architecture like Bitcoin is lacking.

Finally, abilities inherent to the blockchain like its immutability should also

be mentioned although this specific ability could be counted both as a perk and a disadvantage dependent on specific use cases.

4.2.2.1 An implementation of circle of trust

The Circle of Trust model could be beneficial for a select group of entities desiring a blockchain, the following will be a hypothetical scenario describing an implementation of the CoT model.

Imagine that five companies named from A to E decide to start a communal platform designed to exchange insurances between themselves. They could in this case collaborate to construct a CoT blockchain usable to trade data, additionally they could invite the government agency charged with overseeing the insurance sector as a member in the CoT. Through using such a structure transactions could be made almost completely automated as long as the rules regarding transactions were unanimously agreed upon during the creation of the CoT.

A transaction in a CoT system could depending on the blockchain implementation used during its construction work in a multitude of ways however this walkthrough will consider a blockchain consisting of smart contracts like Ethereum or Hyperledger. When a transaction of an insurance is started a customer would contact their insurance company and inform them of their desire to move to another company. Depending on the company, customer contact could either be through an employee or quite possibly a form on the companys' web page. When the transaction is initiated the proceeding step would be to send the collected customer data to a smart contract in charge of facilitating insurance transactions. At this point the functionality of the contract could vary dependent on multiple factors like insurance type or the companies whom the exchange is between. Something general for all the insurances would however be that at this point a validation process is started where the trade information is reviewed and confirmed. Once the data have been validated the trade will be accepted and stored on the blockchain and a confirmation would be sent to the customer.

4.2.3 Permissionless ledgers and an off-chain network

One approach when constructing a blockchain-based architecture is though an off-chain network. The idea behind an off-chain network is to incorpo-

rate beneficial characteristics from solutions currently used in centralisation into a blockchain-based architecture. By doing so the system could be crafted in a way that retains the beneficial characteristics from both centralisation and decentralisation allowing them to complement each other in order to get the best of both worlds.

The most evident problems with the blockchain technology is currently the troubles of overcoming privacy regulations and most prominent amongst them is GDPR. By combining the blockchain in conjunction with an off-chain network, data could be computed both on and off-chain. It is believed that centralised techniques already successful in achieving privacy could yet again be applied to support the blockchain in overcoming similar issues.

One of the largest problems facing the blockchain when trying to achieve GDPR compliance is the technology's use of immutable data. The blockchain intends to represent an immutable receipt recording all occurred transactions such that any peer could trace a certain transaction making it difficult to comply with the law "Rights for erasure". By incorporating an off-chain network computations and storage could also occur off-chain allowing the ability for data to be mutable.

4.2.3.1 An implementation of an off-chain network

To postulate an example of how the system could operate whenever a transaction is issued, the participants in the network attempts to verify the integrity of the transaction, as soon as consensus is achieved the transaction would get stored. The blockchain in this particular system would play the role of a software connector. Where the ledger itself would store transaction pointers, whereas data regarding the transaction would be stored using an off-chain database solution to enforce the idea of mutable data in order to prepare the system to face GDPR requirements. By doing so all data regarding the transaction could be removed apart from the initial transaction pointer which would just represent an arbitrary identifier. Considering the identifier no longer possess the ability to identify any personal data connected to said transaction, the pointer would fit the criteria of a "quasi-identifier" as stated in article 29 of the Data protection working party regulation [30].

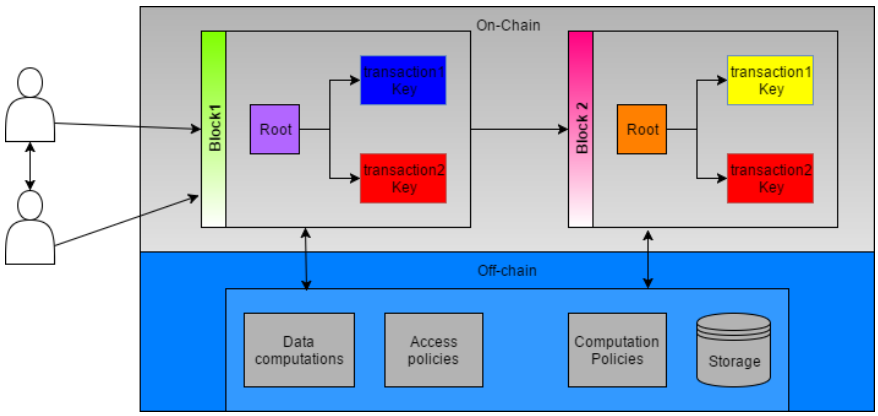

Figure 4.2: An illustration of an off-chain network.

By constructing a system this way using a permissionless ledger some evident flaws will be displayed, especially for industries actively addressing personal related data. Considering permissionless ledgers are constructed by a network of peers collaborating under pseudonyms, there is a possible scenario of peers joining forces to assert control over the system, if this collective group of miners were to take possession of the system they could potentially prevent transactions from being verified. This could wreak havoc regarding laws concerning time constraints like chapter three paragraph two of FAL [12] governing the insurance sector.

A quagmire that would occur if transactions are blocked is a dispute of when an insurance should be considered issued, should it be when the customer sends the request or when it has been verified. In the case of the latter an insurance company could potentially be prevented from ever finding out that a user is insured under their organisation causing legal issues regarding payments.

To relate back to previously mentioned use cases from the purpose chapter into account, a scenario in which a user attempts to change their insurance company would have functionality similar to those used by contemporary centralised solutions. The user would start by issuing a request to change their insurance company to the system. Seeing as this is a time constrained operation due to the risk of having an insurant being uninsured for a longer period of time, this is a scenario in which the dispute of when a consumer should be treated as insured could occur. In the first case the

user would be insured and the request would be verified and stored on the blockchain and data required to be mutable stored in the off-chain storage, in the latter case the transaction would perform the same process however the verification would have to be executed before the insurant would become insured.

Finally to ensure the possibility for governments to have an overview, the government must be granted additional security tools like certificates, making a permissioned ledger more suited for the particular use case. Considering the government would otherwise be required to participate in the network as if they were any participant, meaning the system has not accounted for governance at all.

4.2.4 Permissioned ledgers and an off-chain network

This particular model would work in a similar fashion to previously mentioned models, however the issue of pseudonymity is combatted by switching to a permissioned ledger incorporating the structure and ideas mentioned under the CoT solution into the previously mentioned solution.

By peers collaborating using known identities where in a network where organisations/peers have to reach consensus in order to include participants an innate trust could be created. Additionally, it removes the opportunity for anyone to participate in the network to gain access to data from their peers.

As mentioned the lack of privacy is a hitherto undeveloped field in solely blockchain-based architectures, as shown in the previously mentioned models. However, by Guy Ziskind et al [27,28] as well as Ahmed Kosba et al [5] propose solutions to retain privacy using techniques from centralised systems. So far the blockchain technology have shown no capability to cope with privacy issues, however several models using techniques from centralisation have attempted to address the privacy issue. Previously mentioned models addressed the lack of privacy using external methods outside the scope of the blockchain however both had evident flaws. By combining the previously postulated models, some strengths could be gained and weaknesses could potentially be more clearly defined and therefore easier to address.

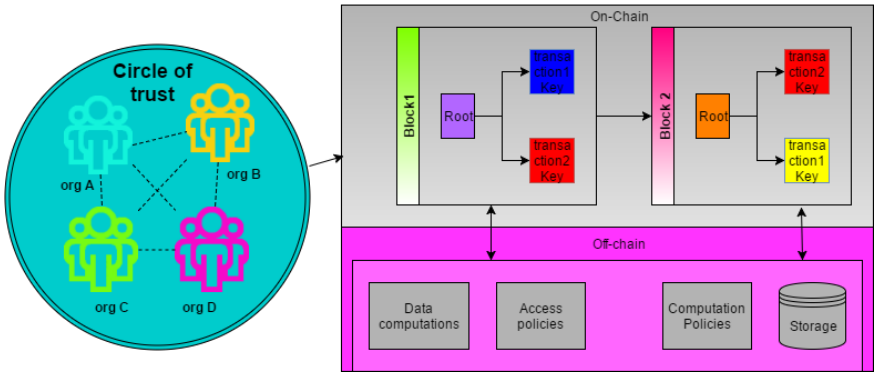

Figure 4.3: An amalgamation of CoT and Off-chain.

By constructing a system that incorporates the idea from previously mentioned models the concept of a CoT could be applied to create an innate trust whereas the off-chain network allows for a performance enhancement while being able to cope with privacy regulations using solutions currently applied in centralised systems. However, all strengths possess some weaknesses, arguably one of the most interesting things with the blockchain technology is the collaboration amongst miners. By having organisations collaborating with each other the opportunities for monopolisation still remains. The fact that organisations are able to monopolise the system by allocating more resources could potentially represent an even pronounced flaw when considering smaller networks. An approach to combat the issue of monopolising the system, is by representing each organisation with one "verifier/miner" and several computation peers. By doing so a single organisation cannot assert control over the system, considering they could only constitute a minority when attempting to achieve consensus. However, seeing as each organisation only possess one vote the system would require a new incentive for organisations to allocate more resources, beyond the necessary ones in order to contribute to a complete ecosystem. Considering this system is formed for the insurance industry there exists a lack of direct economic incentives therefore, a solution could be for organisations to exchange reviews or reputations of some sort allowing organisations to further market themselves resulting in an innate economic incentive.

4.2.5 A pure distributed ledger system

Another possible solution to combat privacy regulations especially GDPR while using a blockchain-based architecture is through purging the chain and construct a new one at certain time intervals. Considering GDPR only applies when there are no other laws justifying the storage of personal data, data could be stored in the ledger as long as the cause is lawfully justified. In Sweden there are laws regarding payment services and e-commerce justifying this particular cause, these state that personal data is allowed to be stored for a certain period of time. However, when that time has expired, the data will again fall under the category of GDPR allowing a user to invoke the regulation.

A proposed model of a pure blockchain system could be constructed using smart contracts, as mentioned earlier in the paper smart contracts are thought of as an agreement which is represented through a piece of code. This piece of code could be modelled to represent an insurance and the code would be executed on the blockchain as if it were any transaction.

However, the outlined problem with using a solely blockchain-based system was privacy regulations due to the blockchains nature of immutable data and a tamper-proof log the system is troubled when facing challenges such as “right for erasure”. Therefore, an approach to make the system compliant with those rules is to reconstruct the blockchain at certain time intervals.

5. Discussion

This chapter will contain the analysis and thoughts regarding the various blockchain implementation models proposed in the paper. Additionally hypothetical comparisons between strengths and weaknesses of these models and other contemporary systems will be performed as a way of evaluating the possible usage of the proposed models.

5.1 Laws

Considering the rules of GDPR only applies for "personal data", a possible workaround would be through "true anonymisation", meaning it is impossible to connect the data to a certain individual. The lack of "true anonymisation" techniques does however disrupt this possible workaround and "pseudo anonymisation" is considered inadequate to fulfill said requirement. As mentioned GDPR only considers the category of "personal data" which is any data allowing a connection to be made between the data and an individual, hence truly anonymised data would not fall under that category. Previously mentioned models introduced an off-chain network with a storage unit to incorporate mutable data, such that the blockchain would only store identifiers towards the storage unit. GDPR states that unique identifiers stored in the ledger would be treated as personal data as long as it connects the identifier to an individual. However, it is not clearly defined whether an identifier remains personal data after the personal data it is used to identify has been removed.

Hence it is ambiguous whether or not the models constructed using the idea of an off-chain storage to incorporate mutable data such that data could remain portable and removable would be considered compliant to GDPR. Seeing as the models were based around the idea of using the blockchain as a transaction identifier, said models could either succeed in achieving compliance or fail miserably all depending on future interpretations of GDPR regulations.

5.2 Circle of trust

The circle of trust method is at its core rather simple and consists of a blockchain architecture constructed by a select group of members working together to create their own shared ledger.

5.2.1 Inherent abilities from the blockchain

Seeing as the Circle of trust, as implied by the name, requires collaboration between multiple parties some level of trust is necessary for this implementation to function properly. Due to the collective's desire for progression brought by the blockchain implementation this model can to some extent breed a certain level of innate trust brought by the collective desire for functionality. This would generally be considered a strength since it could allow competing companies to collaborate and share information. Naturally there are also possible downsides after all the perceived trust could be exploited by one or more parties in the chain hence the need to only invite trusted parties.

An inherent attribute amongst blockchain-based systems is immutable data, meaning once data have been stored it can not be altered. This could naturally be considered both a strength and weakness depending on the situational usage of the implementation. In many cases immutable data is a desired attribute since it makes tampering with data impossible, preventing manipulation and deception. However as with all strengths the shadow of weakness is apparent and in this case the lack of an option to alter data could pose a considerable problem.

The benefits of immutable data systems varies dependent on use case as such the cases stated in this paper must be taken into account when deciding if immutability is a strength or a weakness. If the transaction use case is considered, the advantages of immutability is that all data could act as an eternally unchanging receipt stored on the blockchain creating a ledger of transactional history. In this use case the weaknesses of immutability are few as long as the possible legal conundrums mentioned earlier are disregarded. One possible problem could however be the storage size of the chain, considering data will only ever be added and never removed, the size of the blockchain would only grow and could therefore reach a problematic size.

The other use case to account for is alteration of data at which point the disadvantages of immutability rears its head. Seeing as stored data can not be changed the only way to update the desired data is to store a transaction containing the change. This process requires a rather complicated procedure to be performed to achieve a rather small change additionally the new transaction would have to be stored adding another block to the chain and once again increasing the chain size. A problem that may be even more dire is if the update is not to change data but remove it, due to the fact that data already stored on the chain can not be manipulated it can not be removed. This means that even if an individual wishes to remove all their stored data, the former blockchain members data would remain which could constitute a problem. All these previously mentioned factors does give the CoT architecture an impressive ability to maintain records and history of all transactions however, when the additional potential legal problems are taken into account, immutability could render these advantages rather evanescent.

Another attribute prevailing throughout systems based upon the blockchain structure is their inherent transparency. Through the continuous distribution of blocks amongst the participants, the chain data is propagated throughout the system allowing universal access for any peer. This specific attribute is arguably the greatest strength and weakness of any implementation based upon the blockchain architecture. The transparency allows for any participant to check data stored in the chain to confirm its validity, however this also grants all members access to data on the chain. This specific attribute can as mentioned be considered both positive and negative depending on the situational usage. In any case where general access to all information is counted as a benefit the strength of transparency is apparent. However, in cases where private or secret information is to be stored transparency could have a detrimental affect on the system. Once again the papers specific use cases must be taken into account when deciding if the transparent ability is a strength or weakness.

When regarding the use case of transactions transparency could be beneficial during the validation phase, since all data will be available it is possible for any CoT member to verify the validity of transactional data. Additionally it could be interesting for CoT members to track movement of customers between companies to for example measure the efficiency of an advertisement campaign. The downside of transparency is naturally the lack of privacy, this is not only a legal conundrum but could also prove problematic for companies since their competition could possibly exploit

their customer information. Once again the strength and weakness of an ability possessed by the CoT are rather comparable until legal issues are considered at which point the lack of privacy could prove fatal to a system since some data is required by law to be private. When the use case of updating data is taken into account the benefits or downsides of transparency seems negligible, once again the largest problems would most likely relate to competing parties having access to the data.

A possible weakness of the CoT model is the lack of mining incentive amongst the participants using the circle. Systems like Bitcoin use monetary gain to encourage mining collaboration between participants and in doing so propagating the construction of a chain. In a system build by multiple participants, having a mining system based on monetary gain could prove to be detrimental and end up undermining the trust gained through the cooperation. As such another possible solution to the mining process would be required, the options are many ranging from co-owning a mining central to some kind of inhouse reputation currency used as reward. Another possible solution could be to have a kind of neutral governing entity overseeing the system and acting as a miner, this would however reintroduce third parties.

Finally there are some weaknesses prevailing throughout all systems based on the blockchain architecture. Probably the most apparent weakness is the speed for which data is stored and propagated. Seeing as the propagation of the data as well as the acceptance of new blocks requires substantial network traffic, the storage of data will be slower than in an in-house data center where information can be shared though faster mediums.

5.2.2 Abilities from circle of trust

Using the innate trust created through the usage of the CoT makes it possible for various parties to collaborate and share data while reducing the fear of deception. However, this will only work if all participants in the circle can trust each other as such an implementation of this model could be hard to achieve, there are however a few possible exceptions. Following will be a possible scenario where the CoT model could be applied and an evaluation of this application compared to the systems currently in use.

Let's say a customer wishes to transfer an insurance from company A to company B using the traditional method, a cumbersome manual process would ensue, as explained in the results chapter. However if the compa-

nies were using a model of the CoT to trade information the process could be changed to be mostly automatic. Below a hypothetical transaction process using a CoT will be explained after which it could be compared to the method currently in use.

As the customer starts the transaction process company A receives the request, at this point an employee could simply start an automatic transaction process. This process could be responsible for gathering the user data required for the transaction as well as sending a request for creating an insurance with company B. When the data has been gathered and company B has accepted the insurance request the transaction could simply be stored on the blockchain. By performing a transaction this way not only will much of the manual labour for employees be removed but additionally the blockchain will store the transaction history and information required by the insurance companies. Through using a blockchain as the transaction medium the possibility to track transferals of insurances and the accessibility of customer data will allow companies greater control and understanding of consumer patterns. Finally it should also be considered that depending on the blockchain technology used as a base for the CoT the possibilities can vary greatly; hypothetically if the chain consisted of smart contracts it would be possible to automate the entire process.

The possible gains of a system constructed with the CoT when compared with a legacy system could be many, a more interesting question though is how would a blockchain based system compare to a newly developed centralised system. This however would require substantial research seeing as these kinds of systems are currently being developed behind closed doors by insurance companies and is as such recommended for a future work.

5.3 Distributed ledgers and off-chain networks

Blockchains, or permissionless ledgers as they are often referred to, have as mentioned earlier, no solutions to comply with privacy regulations on their own. Off-chain networks were introduced to allow the technology to incorporate techniques from centralised systems and in doing so privacy could be retained.

5.3.1 Implementations of blockchain and off-chain networks

An architecture structured with an off-chain network would function in a similar manner to systems currently in use, apart from the fact that the exchanges, negotiations and transactions would use the blockchain rather than a “third party”. The blockchain would act as a software connector playing role as a "third party", considering all transactions are validated through the blockchain. As mentioned earlier the off-chain network were introduced to play the role of a storage and computation unit, to support the blockchain with performance issues as well as privacy compliance issues. In regards to the use cases in the purpose chapter, adding an off-chain network would ease the implementation of data alterations considering one of the core ideas of introducing the off-chain network were to incorporate mutable data.

Off-chain network and hybrid systems in general have portrayed a middle ground where centralisation and decentralisation can collaborate and support the blockchain technology to handle privacy compliances, while preserving the integrity of a tamper-proof receipt in the ledger. One of the inherent attributes an off-chain network could cope with is the ability to compute and store data off-chain in a manner similar to how contemporary cloud systems work. In doing so strengths of immutable data could be retained considering the off-chain network could deal with data requiring mutability.

In the other use case where an insurant desires to change its insurance company, the off-chain network would not support the blockchain with any necessary functionality to perform the transaction itself considering the transaction could be performed on a technical basis using smart contracts. It could however support the blockchain in privacy regulations making it applicable on a legal basis. Beyond privacy regulations the off-chain network also helps with mutable data which have proven to be a necessity to achieve privacy of personal data additionally computations constituting in a performance enhancement.

5.3.2 Strength and weaknesses with off-chain networks

As mentioned earlier the strength of the off-chain network often relates to techniques from both centralised and decentralised systems being able to

collaborate. This in turn would allow the system to retain benefits from immutable data, while introducing an opportunity for data to remain mutable. Another strength of the off-chain computation is the performance gain considering hybrid systems are able to execute computations off-chain in a manner similar to distributed systems, making them more comparable. However a blockchain-based system in the current state will most likely not achieve the same performance as distributed systems based on centralisation are able to, considering adding an off-chain network would not relinquish peers from performing computationally heavy tasks required by the blockchain.

All strengths comes with flaws or weaknesses, a particular flaw relating to blockchain-based architectures in general is the ability to cope with time critical assignments. Earlier in the paper the issue of performance were outlined, however the insurance industry is not as dependent of the capability to process a substantial amount of transactions, instead an interesting factor relates to addressing particular transactions under time constraints. For example the law FAL states that a consumer attempting to get insured must have their request issued within a day. An additional flaw in systems based on blockchain architecture involves miners collaborating to assert dominance over the system. To some extent this issue could be solved through a CoT, seeing as peers collaborate under known identities, producing an innate trust.

5.3.3 Comparison to other solutions

In comparison to current solutions in the insurance industry where transactions are carried out mostly through a manual process, a blockchain-based architecture could be able to support organisations in easing this process. However there are several flaws using a blockchain system in practice, considering organisations would have to collaborate with their opposition which is rarely present in the competing institutions.

Additionally in regards to applying a permissioned ledger without the addition of an off-chain network, the ability to incorporate privacy in the system becomes a more challenging task considering the blockchain have shown no signs of achieving privacy on its own. A method to ensure that data is restricted from their respective peers is through encryption, however that would not be a complete solution, considering encryption possesses the disadvantage of being computationally infeasible to decrypt rather than impossible.

The combination of an off-chain network in conjunction with a permissioned ledger appears to have most beneficial characteristics seeing as it manages to retain most of the strengths from having immutable data, while combating disadvantages by incorporating the capability to possess mutable data off-chain. Hence the blockchain could still be applied as a receipt where transactions remain traceable, however sensitive data could retain the opportunity to be portable or removed such that privacy compliances could be achieved.

5.4 A pure distributed ledger system

As described in the previous chapter a possible workaround GDPR using a pure-blockchain architecture, considering there are laws and regulations justifying storage and processing of personal data within a certain period of time. Hence, it is possible to only keep data for as long as it is legal and when the allotted time expires a blockchain could be rebuilt excluding the expired block.

Purging blocks in the blockchain and reconstructing in the interest of overcoming GDPR has both advantages and flaws. Arguably the greatest advantages is the performance, considering a reconstruction of the chain would exclude past blocks, a smaller chain would need to be replicated amongst peers, constituting in an enhancement of performance. Additionally the blockchain could be combined alongside an off-chain network allowing parts of a transaction to be stored off-chain constituting in a smaller amount of data being stored in the ledger allowing for more opportunities of performance enhancement.

However all perks regarding performance comes with a price, purging the blockchain would negate several strengths the blockchain has to offer. Considering one of the arguably greatest advantages of the technology is the tamper-proof receipt recording transaction data, using the purging method would remove the advantage of a unchanging historic record.

5.4.1 An implementation of a pure blockchain-based architecture

A blockchain modelled this way could be represented in several ways, an interesting approach could be for each insurant to construct their own

ledger with several insurance companies, where only their own insurances would be stored. Meaning the model would become reminiscent of a CoT model constituted by parties of interest. Considering smart contracts are represented as a piece of code, a smart contract could be modelled to become an insurance agreement between companies and an insurant.

To reconnect with previously mentioned use cases where the insurant intends to change insurance company or alter said insurance. In the first case where an insurant intends to change insurer, the insurant would issue a request as usual towards the blockchain were included parties would have to verify the transaction and store the transaction on the blockchain. In the latter case, the insurant would go through a similar procedure where the insurant issues a request to alter an insurance by constructing a transaction containing the desired change. The change would then be verified by the other participants in the blockchain network and get stored on the blockchain.

5.5 Impact on society

The blockchain is an astonishing technology with immense potential to revolutionise the digital market however, the technology is currently overshadowed by the fact that it has difficulties in overcoming laws and regulations. The laws and regulations are currently structured around centralised systems where compliance appears to have a negating effect on the blockchain. A game changer for the blockchain technology would be if smart contracts could become legally binding. This could allow smart contracts to justify processing and storage of personal related data in regards to GDPR in a more natural way, rather than a workaround.

Currently the technology is constrained by the fact that contemporary laws and regulations are revolving around centralised systems. The state of Arizona have embraced the idea of digital exchanges and taken a step forwards by making smart contracts legally binding as shown in article 5 HB2417 [31]. By doing so the technology would be able to construct smart contracts which are legally binding leading to the technology being able to move forwards on a legal ground as well as a technical ground. If several countries were to follow this path the possible use cases for the blockchain technology could immediately expand immensely.

A possible example of smart contracts being legally binding is the fact

that a group of organisations or people could join forces and by using a blockchain they could through some smart coding construct their own "insurance company".

Through the usage of smart contracts creating private insurance contracts or simple retirements funds could be possible. By having members of the chain paying a monthly fee, money could be stored in a bank account and when a member reaches retirement age the contract could start paying them money. Through such a simple structure a retirement fund could be created. An additional perk gained if the only action taken by the hypothetical fund was storing money it received in a bank account is that the overhead costs like management fees would drastically decrease giving retired individuals more money. This would not only be an economic effect but could influence society as a whole considering individual economic contracts could be formed between parties removing the need for management parties and as such saving money on a personal basis. Although banks would most likely dislike this kind of development since they would probably lose out on considerable amounts of money they usually obtain through acting as middle men.

Regarding ethical and environmental problems the possible impact blockchain technology could have is seen as negligible. The blockchain technology could be used to create some sort of production line keeping track of resources used during the production and distribution of goods. The production line could have an positive environmental effect, however it would most likely need external assistance in the form of human controllers enforcing and confirming the origin of resources to function properly and is as such not dependant on only the blockchain. An ethical aspect of using the blockchain could be the prevention of fraud through the permanent receipt provided by the technology. However this would most likely also require external assistance for both enforcement and detection of deception and would as such not solely be based on the blockchain technology. To conclude the blockchain may be of some assistance when regarding ethical and environmental problems however the possible use cases seem to mostly be supplementary to a manual human controlling process.

6. Conclusion

As it stands the likelihood of blockchain technology replacing the systems currently in use appears unlikely, considering the still unresolved issues revolving implementations of the technology. When working with personal data the need for confidentiality arises especially if said data could be sensitive for an individual's well being like health records. Since the insurance business often handles sensitive information regarding individuals all their data processing including transactions must posses the ability of privacy. In its current state privacy is something that the blockchain technology is incapable of properly handling, as such the technology still seems unready for real world implementations. However, if hybrid systems combining concurrent centralised systems with a blockchain were to be further developed they could probably find their place in the competing market. Seeing as hybrid systems brandishes multiple advantages when compared to pure centralisation the opportunity for usage certainly exists. Pseudonymity and off-chain storage solutions lends centralised capabilities to blockchain systems giving them the functionality to achieve transactions possibly compliant with GDPR regulations albeit with some cumbersome system conditions. Off-chain solutions lends blockchain the capabilities of privacy and mutability making it capable of lawful transactions and data manipulation however the historic functionality of the technology is also potentially lost. Additionally the decentralised structure of the blockchain lends multiple advantages, like data distribution of transactions between corporations or departments. Currently the largest problem already sighted on the horizon is the continuous arrival of new rules and regulations restricting technologies used within their respective sectors. As technologies must be adaptive and malleable to handle continuous changes in laws the blockchain technology has simply not yet been developed and explored enough to handle such scenarios.

6.1 Future work

Considering this study were conducted before the release of GDPR and potential changes in the Swedish "Dataskyddsförordningen" it was found unnecessary to create an implementation. Therefore verification of the proposed models have yet to be done hence whether or not they could fulfill varying requirements from different laws is unknown. As such an implementation is required in order to verify if the models are capable of fulfilling desired requirements from GDPR and other laws.

Additionally this study only accounted for laws affecting the Swedish region, hence a progression for this study could be to explore how the models cope with laws outside the Swedish region.

Interesting topics to keep in mind for the blockchain technology would be if more countries embrace the idea of making smart contracts legally binding, considering that would allow smart contracts to justify processing, storing in regards to privacy regulations such as GDPR. This would result in a scenario in which the blockchain would be able to be applied in the digital world in a more natural way, rather than having several of its best aspects negated, due to attempts in achieving compliances designed around centralised systems. By having smart contracts legally binding several new applications could be constructed and the possibilities for the technology would be immense.

Another progression for the technology would be if techniques for "true anonymisation" were to be discovered. "True anonymisation" would be a possible workaround from the privacy regulation GDPR allowing the blockchain technology to yet again be applied on its own and have its best aspects shine through, rather than being negated.

Bibliography

[1] Khanna A. Straight Through Processing for Financial Services: The Complete Guide (Complete Technology Guides for Financial Services). Academic Press; 2010.

[2] Bitcoin: A peer-to-peer electronic cash system, 2008; 2012. [Collected: 2017-05-02]. http://www.bitcoin.org/bitcoin.pdf.

[3] Buterin V, et al. A next-generation smart contract and decentralized application platform. white paper. 2014;.

[4] Czepluch JS, Lollike NZ, Malone SO. The use of block chain technology in different application domains. The IT University of Copenhagen, Copenhagen. 2015;.

[5] Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: Security and Privacy (SP), 2016 IEEE Symposium on. IEEE; 2016. p. 839–858.

[6] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on Ethereum smart contracts. Cryptology ePrint Archive: Report 2016/10/07, https://eprint.iacr.org/2016/10/07; 2016.

[7] Ekblaw A, Azaria A, Halamka JD, Lippman A. A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data; 2016.

[8] Linn LA, Koo MB. Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research;.

[9] Hardjono T, Shrier D. Core Identities for Future Transaction Systems. 2016;.

[10] The Swedish Financial Market; 2015. [Collected: 2017-05-02]. http://www.riksbank.se/Documents/Rapporter/Finansmarknaden/2015/rap_finansm_150813_eng.pdf.

[11] Försäkringsrörelselagen; 2010. [Collected: 2017-05-05]. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forsakringsrorelselag-20102043_sfs-2010-2043.

[12] Försäkringsavtalslagen; 2005. [Collected: 2017-05-05]. http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forsakringsavtalslag-2005104_sfs-2005-104.

[13] General Data Protection Regulation, Official Journal of the European Union; 2016-04-27. [Collected: 2017-04-12]. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

[14] Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses; 2012-01-25. [Collected: 2017-05-25]. http://europa.eu/rapid/press-release_IP-12-46_en.htm.

[15] Kadenic V. Compliance of Data Lake Enterprise Architecture Model with the General Data Protection Regulation (GDPR); 2015. Validerat; 20150817 (global$_s tudentproject_s ubmitter$).

[16] Bozic N, Pujolle G, Secci S. A tutorial on blockchain and applications to secure network control-planes. In: Smart Cloud Networks & Systems (SCNS). IEEE; 2016. p. 1–8.

[17] Tai S, Eberhardt J, Klems M. Not ACID, not BASE, but SALT;.

[18] ALBERTSSON A, WENDEBERG R. Emerging Innovations in the Swedish Financial System;.

[19] Kiayias A, Koutsoupias E, Kyropoulou M, Tselekounis Y. Blockchain mining games. In: Proceedings of the 2016 ACM Conference on Economics and Computation. ACM; 2016. p. 365–382.

[20] Yermack D. Corporate Governance and Blockchains*. Review of Finance. 2017;21(1):7. Doi: 10.1093/rof/rfw074. Available from: http://dx.doi.org/10.1093/rof/rfw074.

[21] Franco P. Understanding Bitcoin: Cryptography, engineering and economics. John Wiley & Sons; 2014. ISBN: 9781119019169, doi: 10.1002/9781119019138.

[22] Kapoor B, Pandya P, Sherif JS. Cryptography: A security pillar of privacy, integrity and authenticity of data communication. Kybernetes. 2011;40(9/10):1422–1439. Doi: 10.1108/03684921111169468.

[23] Almuhammadi S, Neuman C. Security and privacy using one-round zero-knowledge proofs. In: Seventh IEEE International Conference on E-Commerce Technology (CEC'05); 2005. p. 435–438. Doi:10.1109/ICECT.2005.78, ISSN: 2378-1963.

[24] Hearn M. Corda–A distributed ledger. Corda Technical White Paper. 2016;.

[25] Brown RG, Carlyle J, Grigg I, Hearn M. Corda: An Introduction. R3 CEV, August. 2016;.

[26] Lagen om betaltjänser; 2010. [Collected: 2017-05-18]. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2010751-om-betaltjanster_sfs-2010-751.

[27] Zyskind G, Nathan O, Pentland A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In: 2015 IEEE Security and Privacy Workshops; 2015. p. 180–184. Doi: 10.1109/SPW.2015.27.

[28] Zyskind G, Nathan O, Pentland A. Enigma: Decentralized computation platform with guaranteed privacy. arXiv preprint arXiv:150603471. 2015;.

[29] Xu X, Pautasso C, Zhu L, Gramoli V, Ponomarev A, Tran AB, et al. The Blockchain as a Software Connector. In: 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA); 2016. p. 182–191. Doi: 10.1109/WICSA.2016.21.

[30] Data protection working party; 2014. [Collected: 2017-05-25]. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[31] signatures; electronic transactions; blockchain technolog; 2017. [Collected: 2017-05-25]. http://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf.

Personal references

[32] Interview with Lawyer Vonne Laan to gain insight in privacy aspects typically related to the blockchain technology [Conducted:2017-05-19].

[33] Questions with Mattias Andersson questions regarding GDPR and different Swedish laws, as well as the current compliance status of the proposed models [Conducted: 2017-05-22].

[34] Interview with Jacob Funck to define the scope and definition of the thesis as well as gain insight in general knowledge regarding the insurance market and the blockchain technology [conducted: 2017-03-28].

[35] Interview with Jacob Funck to gain insight in the current Swedish insurance market [conducted: 2017-05-23].

Appendix

These are questions asked during the interviews with invdividuals experienced within fields of interest:

Is personal data allowed to be stored on the blockchain if it is stored as proof of a transaction? Considering invoking the rule "rights for erasure" would mean that the existence of the transaction would be removed if a participant have the opportunity to remove its existence from the transaction.

How is GDPR evaluated in regards to other laws, so if another national or eu law contradicts a rule stated by GDPR which rule will be applied first?

According to GDPR unique identifiers should be treated as personal data, an example GDPR gives is ip-addresses and mac-addresses, how would a key which is able to identify an entry in an external database be treated?

Will GDPR replace current regulations or will there be adjustments in current regulations such as "dataskyddsförordningen" in order to complement GDPR?

How does pseudonymity work in comparision to true anonymity in regards to GDPR? Considering techniques for "true anonymity" appears non existent with today's technology.

If a key-identifier were to be treated as personal data, would its status as personal data remain if all data whom it identifies were to be deleted?

What would you say is the benefits of using a blockchain implementation in comparison to systems currently in use?

Currently the blockchain is not ready to deal with privacy issues, one way to solve this particular problem is by introducing an off-chain network allowing techniques currently used in centralised systems to be implemented however it appears as if the off-chain network would negate some of the strengths with the blockchain what is your take on this subject?

Another possible solution for the blockchain technology to achieve GDPR compliance is by recreating the blockchain at certain time intervals such that the blockchain does not possess any transactions which are not legally justified to be stored in the ledger, however that would remove the strength of having an eternally unchanging transaction history the benefits however would be that a smaller chain would be replicated do you find this particular trade off worth considering?

TRITA STH 2017:37