Blockchain technology in Scania Services

An investigative study of how blockchain technology can be utilized by Scania

Jim Lindberg
Abstract

Blockchain technology in Scania Services

Jim Lindberg

Blockchain technology emerged in 2009 together with the introduction of Bitcoin, the first virtual currency which enabled nodes in a network, that do not necessarily trust each other, to exchange digital value without the use of trusted intermediaries. Since then, the idea of disintermediation and decentralization has gained traction in a large number of applications outside the world of finance and virtual currencies. This thesis is written in collaboration with Scania, an automotive industry manufacturer, with the purpose of gaining a better understanding of blockchain technology and how it can be used in the transportation industry.

This thesis proposes five potential blockchain use cases that aim to either enhance Scania’s existing services or to create new services. Out of these five use cases, one is deemed inappropriate in regards to the use of blockchain technology while the other four have potentials benefits. The common denominator among these use cases is that they are decentralized in nature meaning that the use of intermediaries is mitigated. It is recognized that all use cases could be implemented using traditional, centralized databases and that the use of blockchain boils down to a technology choice with its own trade-offs relative to other potential choices. This thesis concludes that blockchain technology offers a new kind of database architecture, the main benefit of which is that it lets several non-trusting entities agree on a common set of facts, without having a trusted intermediary establishing these facts.
Summary

The activity of sending digital value between two parties has historically been dependent on a trusted intermediary facilitating the transfer of ownership. In the case of sending money over the internet, banks typically act as trusted intermediaries by making sure that no one can send money they do not have and that the decrease of funds in the sender’s account equals the increase of funds in the receiver’s account. On the other hand, the transfer of physical cash, between two individuals standing next to each other, requires no such intermediary. In computer science terms, the transfer of digital value is made using a client-server architecture whereas the transfer of physical cash is made using a peer-to-peer architecture. Researchers have for a long time tried to realize the concept of peer-to-peer value transactions in the digital space but it was not until 2009, when the cryptocurrency Bitcoin first launched, that digital value could be sent from one party to another, without the use of a single trusted intermediary.

The innovation of Bitcoin is nothing short of spectacular and the full ramifications of this new type of digital asset are yet to be discovered. Even now, the impact has been significant with a whole ecosystem having been built around Bitcoin and similar cryptocurrencies which have emerged by using the same technology that underlies Bitcoin. This technology is known as blockchain technology which meaning can be conceptually described as a data structure, called a blockchain, being replicated over multiple nodes in a network in which there are predefined rules that ensures the blockchain’s consistency over all nodes. Blockchain technology essentially allows several parties, that do not necessarily trust each other, to share a common database, without having a trusted intermediary running this database.

A system dependent on a trusted intermediary can be called a centralized system. The notion of removing the trusted intermediary is called disintermediation. Disintermediation enables a decentralized system in which nodes communicate with each other directly rather than through a single entity as is the case in a centralized system. The number of benefits associated with a decentralized system relative to a centralized system depends on the application in question. In general, decentralized systems have the potential to be more robust as there is no single point of failure in the network. As of lately, the concept of decentralized applications has gained serious interest from many other industries than just finance. One of these industries is the transportation industry in which Scania, an automotive industry manufacturer, operates. The goal of this thesis was to research how Scania can utilize blockchain technology to either enhance current services offered to customers or to create new services.

A total of five use cases related to blockchain technology was identified through internal interviews within Scania’s organization. In the end, one of the use cases was deemed infeasible in relation to blockchain technology while the other four have potential to benefit. The first use case is about Scania having its own decentralized currency which can be used by customers to buy services from third party agents. The second use case relates to an activity called platooning in which trucks drive in close proximity to each other. The benefits of platooning include
savings in fuel consumption. These benefits are not evenly distributed among platooning participants which is why the use case discusses a decentralized system wherein the benefits of each platooning participant are recorded. The third use case is a decentralized provenance tracking system in which goods such as spare parts can be tracked in a supply chain. The fourth use case is a decentralized system for sharing valuable data among competitors within the transportation industry. This use case enables users to share data in exchange for some type of payment. The fifth use case, ultimately deemed inappropriate to combine with blockchain technology, is about Scania communicating with regulators using a blockchain system.

All identified use cases can alternatively be implemented using a centralized architecture. This thesis made no attempt to conclude whether it is advisable to have the use cases being implemented using a conventional centralized database or a decentralized database powered by blockchain technology. Each use case considered in this thesis is rather a conceptual description of how blockchain technology can be used, not whether it should be used. As often is the case when it comes down to a choice between two different technologies, there is a trade-off inherent to the decision. While blockchain technology has the potential to enable decentralized systems with a higher degree of robustness, it lacks in performance and confidentiality when compared with its centralized equivalent.
Table of contents

1. Introduction .............................................................................................................................................. 1
   1.1 Problem discussion .......................................................................................................................... 3
   1.2 Thesis purpose ............................................................................................................................... 3
   1.3 Delimitations ..................................................................................................................................... 3
   1.4 Acknowledgement .......................................................................................................................... 3

2. Background ............................................................................................................................................ 4
   2.1 Decentralized storage ...................................................................................................................... 4
   2.2 Decentralized identification ........................................................................................................... 5
   2.3 Decentralized provenance tracking ............................................................................................... 5

3. Methodology .......................................................................................................................................... 6
   3.1 Analysis model ............................................................................................................................... 7

4. Blockchain technology ......................................................................................................................... 8
   4.1 Bitcoin ............................................................................................................................................ 13
      4.1.1 A bitcoin block ....................................................................................................................... 15
      4.1.2 Transactions .......................................................................................................................... 16
      4.1.3 Colored coins ......................................................................................................................... 18
   4.2 Type of Blockchains ...................................................................................................................... 19
      4.2.1 Public or Private ..................................................................................................................... 19
      4.2.2 Permissioned or Permissionless ........................................................................................... 20
   4.3 Digital signatures .......................................................................................................................... 21
   4.4 Consensus algorithms .................................................................................................................... 21
      4.4.1 Proof of Work ......................................................................................................................... 25
      4.4.2 Proof of Stake ......................................................................................................................... 26
      4.4.3 Mining diversity ...................................................................................................................... 27
   4.5 51% attack ..................................................................................................................................... 27
   4.6 Forks .............................................................................................................................................. 28
   4.7 Blockchain versus a conventional centralized database ............................................................... 29
      4.7.1 Blockchain versus a distributed database ............................................................................. 30
   4.8 Smart contracts ............................................................................................................................. 32

5. Results .................................................................................................................................................. 33
   5.1 ScaniaWallet .................................................................................................................................. 33
      5.1.1 Analysis .................................................................................................................................... 38
   5.2 Platoonning ..................................................................................................................................... 41
      5.2.1 Analysis .................................................................................................................................... 43
   5.3 Provenance tracking ...................................................................................................................... 45
      5.3.1 Analysis .................................................................................................................................... 48
   5.4 Event data sharing with competitors ............................................................................................ 49
      5.4.1 Analysis .................................................................................................................................... 53
   5.5 Transparent communication with regulators ................................................................................ 54
      5.5.1 Analysis .................................................................................................................................... 55

6. Discussion ............................................................................................................................................ 56

7. Conclusion ........................................................................................................................................... 57

References ................................................................................................................................................. 61
1. Introduction

In 2008, a person or group behind the pseudonym Satoshi Nakamoto released a white paper called *Bitcoin: A Peer-to-Peer Electronic Cash System* [1]. This white paper represents the beginning of the story about Bitcoin, the world’s biggest digital currency [2], as measured by market capitalization. By early 2009, the first transaction was made on the Bitcoin network. In 2015, the number of merchants accepting bitcoin for its products and services exceeded 100,000 worldwide [3]. While the value of one bitcoin since its introduction has been volatile to say the least, it has been appreciating heavily in value. From initially being practically worthless, a Bitcoin is today worth approximately 2,374 US Dollars [2].

But what brought Bitcoin to its current state of being a valuable virtual currency? After all, the idea of virtual currencies existed long before Bitcoin with hundreds of academic papers [4] already devoted to the subject without anything coming even close to Bitcoin’s success. The problem with previous virtual currencies were that they depended on trusted intermediaries, much like our banking system. Bitcoin does not have to use trusted intermediaries in the same way and the reason why is called “blockchain”: the technology on which Bitcoin largely relies upon to enable the movement of digital assets in a decentralized, peer-to-peer network in which there is no centralized intermediary facilitating the exchange [5].

Outside the world of Bitcoin, and other blockchain cryptocurrencies which have appeared as a consequence of Bitcoin’s success, electronic payments require a trusted third party, commonly a bank, to carry through a transaction [6]. This third party acts as an intermediary between the two parties wishing to transact. The transacting parties trusts this intermediary with the task of keeping track of the ownership of assets, e.g. making sure that the increase in the receiver’s balance equates to the decrease in the sender’s balance. Blockchain technology, due to certain features that is described in later sections of this thesis, removes the need for a single intermediating entity when conducting electronic transactions [7]. The removal or mitigation of intermediaries is called disintermediation. The average consumer might not initially appreciate the implications associated with the disintermediation of digital value transfer which is understandable considering that conventional payment system in place today work seemingly well for most applications.

But those that have ever wired money overseas, who knows about the expensive fees and delays related to this activity, probably think there is room for improvement. Both the expensive fees and the number of days it takes for money to electronically move from point A to B can be attributed to the intermediaries involved in the transactions. The

---

1 “A cryptocurrency is a digital or virtual currency that uses cryptography for security. A cryptocurrency is difficult to counterfeit because of this security feature. A defining feature of a cryptocurrency, and arguably its most endearing allure, is its organic nature; it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation.” [77]
intermediaries need to be compensated for their work and the more intermediaries involved, and in an international transaction there could be many, the higher the fees. Also, these intermediaries need to coordinate with each other so that the money can move from one intermediary to another and this activity is commonly, for various reasons, only performed at discrete time points, thus the transaction delay [6]. In a peer-to-peer network that relies on blockchain technology, such as the Bitcoin network, where there are no single intermediaries, transactions can be completed in near real-time with fees having the potential to be lower than the ones generally charged in most payment systems today.

One inherent feature of the blockchain technology is that it is distributed over all the nodes in the network meaning that each network participant has its own copy of the blockchain. The distributed aspect of blockchain offers a higher degree of robustness [8] as there is no single point of failure in the network which can be compared to a centralized network where a successful attack on the central node can have adverse consequences.

Blockchain technology enabled Bitcoin to solve a problem not previously solved, namely the problem of sending value over the internet, without having to rely on a third trusted party to intermediate the transaction. Blockchain technology essentially permits network participants to collectively and securely maintain and update a shared database where past records are considered immutable and any change to the database needs to be approved by the network as a whole. Ownership of assets are enforced by the blockchain and all its participants rather than by a central trusted authority. A decentralized network of this kind has the potential to prove useful in a number of applications other than just cryptocurrencies in particular and digital value transfer in general.

When it comes to blockchain use cases outside the world of digital currencies, the financial sector currently receives the most attention. The fact that Bitcoin is a proven financial application itself is arguably why it is relatively easy to extend the idea of blockchain to the world of finance. However, the potential for the blockchain technology extends far beyond payment systems. Potential applications include Internet of things [9] where connected devices would communicate directly with each other rather than through a central server, property registration [10] where records of ownership would be shared in a peer-to-peer network instead of having a central government entity owning and storing the records, and new types of social networks [11] where users own their data as opposed to a third party like Facebook or Google owning it. The list of potential use cases is long and the expectations of what one can accomplish with blockchain technology is high. With well over 500 [12] companies devoted to creating applications involving blockchain, it is difficult to ignore this emerging technology. Despite the number of people and resources dedicated to the purpose of realizing blockchains’ potential value, the technology is yet to reach mainstream adoption. Gartner recently identified blockchain as almost being at the peak of the Hype Cycle [13] which suggests that the expectations may be set too high at this point in time.
1.1 Problem discussion

Blockchain technology has the potential to prove useful in a number of areas other than Bitcoin and cryptocurrencies. The question is which areas can benefit from the technology and how. This thesis is not as much about solving a particular problem than it is to find one to be solved using a predefined solution and where the solution is blockchain technology.

The idea of disintermediation in different applications is interesting due to its potential to save costs, to increase speed, and to reduce single point of failures in various types of network. This thesis aimed to see if the transportation industry can use blockchain technology to improve existing services or to create new kind of services. Since this thesis was written in collaboration with Scania, which is an automotive industry manufacturer of commercial vehicles with a focus on heavy trucks and buses, the area in which to look for blockchain use cases was within Scania’s business.

1.2 Thesis purpose

The objective of this study was to identify several use cases that utilize blockchain technology. These use cases relate to Scania’s business with the purpose of enhancing current services provided to customers as well as creating new services that has the potential to offer value. The identified use cases are finally analysed in regards to their value proposition, complexity and corresponding centralized solution. The purpose of this analysis was to give an idea about which use cases makes the most sense to implement.

1.3 Delimitations

When discussing potential blockchain use cases, no consideration in respect to legal or regulatory aspects has been taken. In terms of the proposed use cases, this thesis merely focuses on providing theoretical explanations of how blockchain technology can be used, not whether the proposed use cases are compliant with current laws and regulations. This delimitation is perhaps most relevant in the use case in which financial transactions are meant to be handled.

1.4 Acknowledgement

Marcus Löf, a student from KTH Royal Institute of Technology, wrote his thesis about blockchain technology in parallel with the author of this thesis. Even though the theses differ somewhat in scope and purpose, a significant amount of discussion has taken place between the authors leading to the possibility of some shared ideas being included in both thesis reports.
2. Background

Scania’s IoT platform consists of several different products that are connected to Scania’s central servers. The connection is established by communication units that sends and receives data via the mobile network. Scania offers their customers different services by using the data from the connected products in a smart way. For example, using data about a truck’s suspension system enables Scania to tailor the maintenance experience for each truck by knowing what components needs to be replaced at which time. This type of service minimizes the amount of generic maintenance that needs to be done on the trucks which ultimately saves the hauliers money. These services are generally of great value for Scania’s customers and they also help the company differentiate its products from competitors’ products. With Scania’s connected vehicles in mind, the use of blockchain technology has been identified as a potential way to further enhance the services offered to customers.

Blockchain technology was invented through Bitcoin with the main innovation being disintermediation meaning that value could, for the first time, be digitally transferred between two parties that do not trust each other, without the need of a trusted third party intermediating the transaction. The notion of disintermediation and decentralization being of value is not exclusive to the world of currencies. Many start-ups are currently trying to use blockchain technology to disrupt industries which relies on centralized infrastructures in which trust needs to be put in individual organizations. With the purpose of concretizing the idea of blockchains outside of Bitcoin, a few current projects are described in the following subsections.

2.1 Decentralized storage

Many organizations and individuals are today using cloud services to store and share their data [14]. Faster internet connections enable the storage of data in remote places, and not necessarily on local hard drives, while still having the data readily available to the user. The use of cloud services has many advantages [15] with cost efficiency and easy access to the data from different devices being two of the most practical ones. One of the possible disadvantages is that users must trust a third trusted party in the form of a cloud service provider to store their data in a secure way. Sia is a company that wants to use blockchain technology to enable a distributed peer-to-peer network that securely stores the data without the need of a trusted third party. Or in the company’s own words [16]:

*Sia leverages the capacity of blockchain technology to enable distributed networks to reach consensus in a secure and trustless way. Cryptographically secured smart contracts ensure the encryption and transfer of data with no possibility for a third party to interfere in any way.*
Sia is a new approach to cloud storage platforms. Instead of all datacenters being owned and operated by a single company, Sia opens the floodgates and allows anyone to make money by renting out their hard drive. Data integrity is protected using redundancy and cryptography.

2.2 Decentralized identification

ShoCard [17] is trying to leverage blockchain technology to store digital identities that enables users to identify themselves without having to use passports or other types of physical identification documents. ShoCard is not really about removing a third trusted party since an identity always needs to be vouched for to be considered valid. ShoCard is more about distributing the ability to issue and verifying identities digitally over several parties. Rather than trusting a single organization, e.g. a government or bank, in regards to a particular identity, ShoCard wants to use a blockchain to enable a user to have its identity easily validated by several organizations. A blockchain in this case is used to record these verifications in an immutable ledger owned by no one but shared by many. A ShoCard user creates an identity on the blockchain using its personal details. For the identity to bear any significance, it needs to be validated, preferably by an organization that is known and trusted for its ability to verify identities. When the user then tries to use its identity to travel for example, the travel agency can search the blockchain and see if the identity has been validated by an organization that it trusts. If that is the case, the travel agency can consider the identity presented as valid. BlockCypher, the blockchain platform that ShoCard uses, write [18]:

...ShoCard created an identity management application that uses public/private key encryption and data hashing to safely store and exchange identity data. This identity data includes biometrics like fingerprints, facial maps, iris patterns, and voice. Through the ShoCard application, a person manages and carries her identity data on her mobile phone. This person is the only person who determines which identification details are shared. ShoCard uses the blockchain as a public, immutable ledger that allows third parties to validate that the original data or certification has not been changed or misrepresented...

2.3 Decentralized provenance tracking

Provenance is a company that wants to use blockchain technology to track the provenance of products and goods. There are often many different entities involved in a supply chain which makes it hard to know where a product is or where it came from. If all actors in a supply chain reports to a centralized database, traceability and ownership tracking could be achieved. However, this type of centralized solution comes with a cost. The entity running the database will want to cover its own costs while also collecting a profit. Furthermore, actors in the network needs to trust the entity running the centralized database. Much like blockchain technology enables bitcoins to be exchanged without the use of a trusted intermediary, blockchain can be used to move digital tokens of “real”
physical goods between actors in a supply chain without the use of a trusted intermediary. In regards to the blockchain technology, Provenance writes [19]:

*Provenance is building a traceability system for materials and products using a new kind of data system called a blockchain. It is a data system for securely storing information - inherently auditable, unchangeable and open. We are working towards an open traceability protocol - that anyone can use to track the provenance of anything from coffee beans to a roll of fabric.*

*Until now centralised data systems were the only way to power a traceability system for materials to ensure data was trustworthy. Blockchain technology changes this fundamentally. We believe it can disrupt how we track the attributes and journey of every material thing - powering a system everyone in the supply chain can be part of.*

3. Methodology

The main methodology to gather information in this thesis has been an extensive literature review using electronic sources. First, a thorough understanding of the blockchain technology was acquired by reading academic papers and articles on the subject. This research was followed by a full day seminar led by individuals carrying knowledge about blockchain technology in general and Bitcoin in particular. After these activities, the lion part of the blockchain technology section was formulated and reflected on. The aim of the blockchain technology section was to gain a good understanding of what a blockchain is and how it can be used, thus creating a solid foundation on which to discuss potential blockchain use cases for Scania.

The second phase of this thesis included meetings with several stakeholders throughout the Scania organization. These stakeholders worked with different areas related to Scania’s services and were therefore able to offer a good view of potential use cases. Due to the thesis author’s limited experience within the transportation industry and its challenges, these types of meetings were essential to gain the necessary understanding required to propose relevant use cases.

The third and last phase consisted of deciding on relevant use cases and subsequently analysing these in terms of their complexity and value proposition. The only requirement for a use case to be deemed relevant was that it could be implemented using a blockchain, not necessarily that it was advisable to do so. The use cases were conceptually described, without going too deep in the technical details needed to implement them, and then analysed using a simple model which purpose was to highlight different aspects of the proposed use case. This model is described in the following section.
3.1 Analysis model

When analysing the different use cases, three different aspects were considered through a model abbreviated CVC. The aspects in question are Complexity, Value proposition and Corresponding centralized solution. The model is neither mutually exclusive nor collectively exhaustive. The model was developed by the thesis author but inspired by the Technology acceptance model (TAM), which was first developed in 1989 by Davis, Bagozzi & Warshaw [20]. TAM suggests that the two main factors influencing the decision about how and when new technology is used are Perceived usefulness; which is incorporated in the CVC model’s Value proposition, and Perceived ease-of-use; which is covered in the CVC model’s Complexity. TAM focuses mainly on end-users such as consumers in the process of adopting a new technology, e.g. the personal computer, while the CVC model is meant to be used as a tool to evaluate which blockchain use cases are most relevant for a company to pursue. The resemblance in context between the two models lies in the theme of new technology while the difference lies in the target of analysis. With the assumption that the behaviour of decision makers in companies resemble the behaviour of end-users to some extent, TAM appears to be a good model to base this thesis’s analysis on. Each identified blockchain use case has been qualitatively evaluated using the CVC aspects which are explained as follows:

- **Complexity** – Complexity refers to the perceived difficulty related to implementing the use case in question. For example; are there existing vendors that offers off-the-shelf software that can be used and if so, how much configuration is likely needed? Decentralized applications powered by blockchain technology are new and not nearly as proven as centralized applications commonly used in many settings today. There seems to be several non-trivial challenges associated with the implementation of decentralized systems. The complexity aspect of the analysis model aims to highlight these challenges. Before pursuing a particular use case, the perceived difficulty related to these challenges need to be put in contrast to the value it may bring to solve them.

- **Value proposition** – This aspect highlights the perceived usefulness of the use case from the perspective of Scania. Does the use case include direct benefits for Scania in terms of lower costs or is it rather about improving Scania’s offer to its customer and thus, value is to be absorbed through higher revenues? Blockchain technology is about collaboration between entities that does not necessarily trust each other. This aspect also discusses how the value proposition and incentives look for different types of network participants with which Scania would need to collaborate.

- **Corresponding centralized solution** – Assuming that everything that can be done using a blockchain can also be done using a trusted intermediary, how does the decentralized version of the use case compare to the centralized version? This aspect discusses the degree of decentralization inherent to the use case and its implications for the system.
The CVC aspects were evaluated qualitatively through reasoning. For each aspect, relevant points were highlighted and discussed. From this discussion, a brief conclusion was made for each aspect (see chapter 7. Conclusion). As the evaluation method contains a degree of subjectivity, the reliability of this research could be in question. In terms of maximizing reliability, a quantitative approach would have been desirable. However, as there are currently few to no working enterprise blockchain applications, it is difficult to find quantitative variables to be measured and compared without developing an application oneself, something that was deemed out of scope since the purpose of this thesis was to identify blockchain use cases that made sense on a conceptual level. An idea for further research could be to create a working prototype for one of the identified use cases. This prototype could then be analyzed quantitatively in respect to, e.g., performance or security.

To increase the research reliability within the realm of qualitative analysis, one could make better use of methods such as interviews or questionnaires which would be directed to experts within the field of blockchain technology. Even though discussion has taken place with knowledgeable individuals within the blockchain space, the conversations were too informal and brief, and the experts consulted were too few, to make a scientifically fully reliable contribution to the written thesis. Furthermore, the meetings with experts at Scania (one expert per use case) could have been formalized as a way to increase reliability. Formalized and consistent interviews with internal experts at Scania would make their opinions of the use cases, in respect to their potential contribution to Scania's business, mutually comparable to a higher degree.

4. Blockchain technology

An early disclaimer is warranted when attempting to pinpoint what the blockchain technology is, as is one of the first tasks of this thesis. As of the time of writing, there exist no semantic consensus regarding what blockchain is and what it is not [20]. Some might say that the term blockchain is still under social construction although the core concepts of the technology seem to be agreed upon, at least to a somewhat satisfactory extent. This thesis will try to be as explicit as possible about the parts of the blockchain technology that have seemingly reached consensus and, in the same spirit, be as transparent as possible about the parts that remain objects of discussion. In the end, the interesting parts for this thesis lies in the usefulness of different technology components, not what exact term should be used for the collection of these components.

One of the things that generates the least amount of contradictory answers, if any, is the origin of the blockchain technology. Even though he referred to the term “block chain”, rather than “blockchain”, in his white paper about the virtual currency Bitcoin that was introduced in 2008, the author(s) behind the pseudonym Satoshi Nakamoto [1] explains the fundamental concept behind the workings of Bitcoin which by large is the blockchain technology. Nakamoto made no attempt to distinguish between the concept of blockchain
and its application Bitcoin, it is rather a task for the individual seeking a clear definition of blockchain as a first step to figuring out how the technology can be used in other applications than digital currencies.

On a high level, a blockchain is a data structure much like a linked list in the sense that each block refers to its preceding block. While data can be added to a linked list in numerous ways depending on its configuration, a new block of data in a blockchain is generally added on top of the last block in the chain. Another difference between a blockchain and a linked list is that a blockchain refers to a preceding element by pointing to its hash value rather than using a pointer to the object itself. Figure 1 illustrates the link (chain) between blocks.

![Figure 1. Illustration of the links (chains) between blocks](image)

The hash value of a block is a function of all the content inside a block. Any change to this content will change the hash in an unpredictable way which in turn will change the hash pointer in the next block which consequently will change that block’s hash value and so on. The propagation of new hash values to subsequent blocks, when a change is made in one block, is illustrated in Figure 2 in which the text string in the second block is changed to “Hi world!” rather than “Hello world!”. A hash function is a so-called one-way function meaning that the input to a hash function cannot be guessed simply by looking at the output. This cryptographic feature is essential in a blockchain and it is one of the things that makes it difficult for a potential adversary to tamper with data recorded on the blockchain because any change in a block will change that block’s hash and all subsequent hashes after it, making it easy to detect when a change to one of the blocks has been made.

![Figure 2. If the content of one block changes, its hash and all subsequent blocks’ hashes changes.](image)
However, this cryptographic feature itself is not what makes the blockchain technology special. For a blockchain to be of value in a wider context, the underlying data structure needs to be coupled with a protocol that enables the blockchain to be maintained in a decentralized environment in which a copy of the blockchain exist in all nodes of the network and where there is a consensus mechanism that enables nodes to agree on the current state of the blockchain [21]. Furthermore, rules need to be clearly defined in this protocol in regards to who gets to create new blocks. Simply chaining blocks of data using hash pointers is thus not enough to be labelled as a blockchain as the term is commonly used today. A blockchain network is a network of computers, referred to as nodes in the remainder of this thesis, which collectively maintains a blockchain.

Blockchains provide cryptographically auditable, append-only ledgers that can be used to build decentralized applications, meaning that users of the application do not need to put trust in one centralized entity. The authenticity and origin of transactions in the network is ensured by a public key infrastructure using digital signatures. [22]

The blockchain technology enables nodes in a network to communicate with each other in a decentralized, peer-to-peer fashion. The difference between a peer-to-peer network and a centralized network, a so-called client-server network, is illustrated in Figure 3.

![Figure 3. Difference between peer-to-peer and client-server infrastructure](image)

Figure 3 illustrates several different advantages with the peer-to-peer infrastructure compared to the client-server infrastructure. First, there is no single point of failure in the peer-to-peer network. If one node goes down, the others will still be able to communicate with each other. The client-server network on the other hand is far more vulnerable. If the server gets attacked or fail for any other reason, the whole network goes down. Second, the peer-to-peer network enable nodes to communicate with each other directly thus removing the risk of the intermediary censoring any communication. Third, in many applications where the client-server network is used, the central node takes a fee for acting as an intermediary between the two nodes. In a peer-to-peer network, nodes can deal with each other without needing to pay a third party to establish the connection.
A blockchain is distributed in the sense that all nodes in the network has a copy of the blockchain. Figure 5 illustrates a blockchain being represented at each node. In a centralized network, every node would just see the data that the centralized authority decides it has permission to see. Moreover, the nodes would have to trust this authority in terms of the correctness of the data. A blockchain, characterized by decentralization and a consensus mechanism that makes sure that every node has the same copy of the blockchain, is often described as trustless as nodes do not need to trust each other to transact with each other.

![Blockchain Diagram]

Figure 4. Every node holds a copy of the blockchain

The reader might find it instructive at this early point in the thesis, and hopefully not confusing, to be served a few concise blockchain definitions as a mean to better understand the essence of what a blockchain is. The initial notion about the lack of consensus regarding the definition of blockchain is trusted to be reinforced by the following list of somewhat different definitions. However, none of the definitions contradict anything noted about blockchain so far in this thesis nor do they contradict each other, they merely have slightly different views on the core of the technology and what is included in it. To be fair, it is difficult to properly describe blockchain in one sentence.

All the sources from which the definitions have been drawn follows up by doing a good job elaborating on the definitions.

1) “Blockchain is essentially a public ledger, in which all committed transactions are stored in a list (or a chain)” [23]
2) “The blockchain is the public ledger of all Bitcoin transactions that have ever been executed” [24]
3) “A blockchain is a sequential database of information that is secured by methods of cryptographic proof, and it offers an alternative to classical financial ledgers” [25]
4) “A blockchain is a type of a distributed database specifically suited for processing time-ordered data such as financial transactions” [26]

5) “A blockchain is a sequence of timestamped transactions, where each transaction includes a variable number of output addresses (each address is a 160-bit number)” [27]

6) “A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong cryptoeconomically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies.” [28]

7) “A blockchain is a distributed database which maintains a list of records, each of which is known as blocks” [29]

The first term that calls for closer inspection is “public”. The first two definitions hints that a blockchain should be public. Public in this sense essentially means that any node should be able to connect to the blockchain network. As will become apparent in a later subsection, the notion of a private blockchain also exists so a question whether a blockchain must be public, or if it also can be private, arises at this point. This thesis recognizes both types as a blockchain but it is important to make the distinction between public and private since it has implications on how the network operates.

Definition 2 refers to “the” blockchain as being the ledger of all Bitcoin transactions that ever have been executed. While the part about a blockchain containing every transaction made on the network is generally true, there seems to be little support behind the idea of blockchain being exclusive to Bitcoin. Bitcoin builds on the blockchain technology and they are indeed inseparable from the perspective of Bitcoin. However, blockchain can exist without Bitcoin. In fact, several other blockchains have already been developed and as of such, there is no such thing as “the” blockchain.

The idea that a blockchain can be considered a kind of database seems to hold true in the eyes of many, as does the idea about it being distributed over several nodes. The notion about the blocks being sequential and time-ordered also seem to enjoy vast support. Definition 6 is the longest definition by far and it is also the one with the biggest scope. It was presented by Vitalik Buterin, co-founder of the blockchain-based platform Ethereum, who is trying to extend the use of blockchain technology beyond Bitcoin through the use of “Smart contracts”, a term which is described in section 4.8.

To further illustrate the confusion regarding semantics, the term “Distributed Ledger Technology”, or DLT in short, is sometimes used as a synonym to blockchain technology. While the overall objective of decentralization is shared by the two terms, they could be seen as two different things. Blockchain technology is a type of DLT. Figure 5 illustrates this relation. While a blockchain is made of hash linked blocks, a DLT application does not necessarily incorporate the blockchain data structure. DLT is a sort of umbrella term
that refers to the ability to share a database between entities that do not necessarily trust each other, without using a centralized authority. Richard Gendal Brown, CTO of a DLT company called R3, defines Distributed Ledgers concisely [30]:

“Distributed ledgers – or decentralised databases – are systems that enable parties who don’t fully trust each other to form and maintain consensus about the existence, status and evolution of a set of shared facts”

The remainder of this section will start off by detailing Bitcoin and how this cryptocurrency functions. Bitcoin is currently the largest virtual currency by market capitalization [2] and by far the best example of a real world blockchain application and that is why this thesis will use Bitcoin frequently as a mean to explain the underlying blockchain technology. The ambition is to separate Bitcoin and blockchain as much as possible but this thesis will inevitably refer to Bitcoin outside the designated subsection as well. The generous use of Bitcoin as an example only serves an educational purpose as it is the most proven blockchain application to date. After Bitcoin has been described, mechanisms that are believed to have a closer relation to the blockchain technology in general, rather than being necessarily related to only Bitcoin and cryptocurrencies, is described more in detail.

4.1 Bitcoin

The concept of blockchain was introduced by Satoshi Nakamoto when he released his white paper [1] detailing Bitcoin; a decentralized digital currency [4]. The first block in the Bitcoin blockchain, the so-called genesis block, was created on January 3rd, 2009 [4].
The idea behind Bitcoin was to enable trade over a communication channel in a peer-to-peer fashion. Peer-to-peer networks have existed for quite some time, but not for the transfer of assets such as money. Data files have for a long time been shareable using different peer-to-peer software. In these kinds of peer-to-peer networks, files are not really transferred from one party to another, the sender rather sends a copy over the network. Both the sender and receiver will subsequently have the file. However, sending a copy becomes troublesome when assets such as money are to be transferred. When making a transaction with money, the additional funds in the recipient’s balance needs to equate to the decrease in the sender’s balance. No one should be able to spend the same money twice. For two parties to electronically send payments to each other, a third trusted party has traditionally been needed to act as an intermediate. In the case of payments using money, a bank or payment processor typically acts as this trusted third party.

When physical cash changes hands, it is essentially a peer-to-peer transaction. In the digital world however, before Bitcoin and blockchain technology, there existed no mechanism to make electronic payments between two parties without a third trusted party. The need for a third party to process electronic payments is problematic, as outlined in Nakamoto’s white paper, mainly because of two reasons:

- The cost of mediation. This cost increases the total transaction cost which limits the minimum practical transaction size and cuts of the possibility for casual transactions [1]. Furthermore, if more than one intermediator is needed, it can take a significant amount of time to perform the transaction. The cost of mediation is illustrated in Figure 6.
- The lack of non-reversible transactions. There is a cost related to the loss of ability to make non-reversible payments for non-reversible transactions [1]. Merchants lose money when delivering a product for which the payment is later reversed due to fraud.
Transactions that are hard to reverse provides a fraud protection for the seller of a product or service [4] while routine escrow services can be implemented to protect the buyer [1]. What Bitcoin does to enforce this irreversibility of transactions is to make it computationally difficult for a transaction to be reversed. It is the underlying blockchain technology that enforces this irreversibility by incorporating a clever consensus algorithm called Proof of Work. The Proof of Work algorithm is described in section 4.4.1.

A bank acting as a third trusted party knows about all the transactions ever made in its network because all the transactions must go through it. It is therefore easy for the bank to see if one party has the required funds to make a transaction because it can check its centralized record to see if there is enough balance on the account. The issue in a peer-to-peer digital currency network of whether a peer has the money it is claiming is non-trivial. In a peer-to-peer network there is no central, trusted authority that holds the answer. Nakamoto concludes that the only way for a peer to know the balance of another peer is to know about all transactions ever made [1]. Since all transactions are recorded on the blockchain, which all nodes hold a copy of, the network can, through the consensus algorithm Proof of Work, agree on how many bitcoins each peer owns. All the blocks in the chain are timestamped meaning that when consensus about the state of the blockchain among the network participants is reached, there is no doubt whether a peer is trying to spend coins it already has spent.

4.1.1 A bitcoin block

Each block in a blockchain contains data. What type of data is a question about implementation. In the case of Bitcoin, each block, illustrated in Figure 7, contains transactions. Other things that are included in each Bitcoin block are [5]:

- The hash of the block
- The hash of the previous block
- Nonce (an integer)
- Timestamp

![Diagram of Bitcoin blocks](image.png)

*Figure 7. High level view of Bitcoin blocks*

When a new block is propagated to the network, all nodes will add it to their respective copies of the blockchain, but only if the block in question is valid. The algorithm for checking if a block is valid performs the following steps [5]:

1) Check if the previous block referenced by the block exists and is valid
2) Check that the timestamp of the block is greater than that of the previous block
3) Check that the Proof of Work on the block is valid
4) Check that all the transactions in the block are valid

If any of the above steps returns false, the block is considered invalid.

### 4.1.2 Transactions

Each Bitcoin transaction contains a list of outputs, which specifies the public addresses that are to receive bitcoins and how many, and a list of inputs that reference outputs of previous transactions [32]. Bitcoin’s transaction model is illustrated in Figure 8. The number of inputs and outputs in the respective lists can be anything from one to several thousands [33]. The initiator of a transaction needs to own all the inputs that are included in it, the transaction will otherwise be considered invalid [4]. By referencing a previous transactions’ output that has not been referenced in a previous transaction, a so called unspent transaction output (UTXO) and by showing through your digital signature that you are the recipient of that output, you prove that you have the bitcoins. The key insight here is that the referenced output has not been spent already, i.e. the UTXO has not already been referenced in another transaction’s input. An issue emerges if a user would like to only partially spent a previously received output. In that case, a question whether the output is spent or not arises.
The way the Bitcoin protocol is set up is that each output must be spent in its entirety meaning that a transaction which input refers to a previous output of, say 10 BTC, must have its own outputs sum up to 10 BTC. If the input value exceeds the output value, the difference will become a transaction fees that will be claimed by the node eventually confirming the transaction and putting it in a block [5], a so-called miner [1]. The transaction fee serves as an incentive for nodes to help confirm transactions. If the user wishes to send only 7 BTC to a certain address, and do not want to post any transaction fee, then it simply sends the remaining 3 BTC to itself. Using this approach, there is no question about whether a certain output has been spent or not. When a previous output has been used as an input, it cannot be used again and hence, it cannot be double-spent [32].

Due to the Bitcoin network being distributed, the input-equals-output mechanism alone cannot prevent double-spending. Transactions do not reach all nodes at the exact same time and therefore, nodes might not be aware that a certain input has already been spend. The adversary trying to double-spend could reference the same output in two different transactions and hope that they both get accepted. Luckily, the consensus mechanism called Proof of Work ensures that all nodes are consistent in terms of the transactions they store and thus, a double-spend is almost impossible. For a user to pull off a double-spend, it would have to control more than 51% of the network. A detailed description about the so called 51%-attack will follow section 4.5.

All nodes in the Bitcoin network has permission to suggest new transactions. These transactions get pooled together in a pool of unconfirmed transactions [34]. For a transaction to be confirmed, it needs to make it into a block that is successfully attached to the blockchain. For the transaction to have any chance of making it into a block, it
needs to be valid meaning it outputs does not exceed its inputs and that there is a proof from the issuer, a digital signature, that it owns all the referenced inputs, the so called UTXOs [4]. The state of the Bitcoin blockchain, i.e. the balance of every user in the network, is represented by all the UTXOs owned respectively [5]. Each block contains the current state of the blockchain with all the UTXOs and its respective owners, in the form of pseudo-anonymous public addresses, specified [5].

4.1.3 Coloured coins

Coloured coins refer to Bitcoins that have been coloured to represent not only the underlying Bitcoins, but also some other real-world asset or alternative digital currency [35]. In the Bitcoin transaction object, there is a data field called OP_RETURN that is empty by default but which can hold an arbitrary piece of data if needed. A coloured coins protocol can utilize this data field to effectively colour bitcoins. For nodes to recognize a specific coin as coloured, they need to have a coloured coin software wallet.

To issue some coloured coins on top of the Bitcoin blockchain, one first needs to have some bitcoins. As previously outlined, Bitcoins in circulation are represented by UTXOs that need to be fully consumed when spent, thus creating one or several new UTXOs. A bitcoin can be divided into pieces as small as one millionth of a Bitcoin, a so called satoshi, meaning that an UTXO worth one bitcoin can at most represent one million outputs, where each output is worth one satoshi. To colour these outputs, the issuer of coloured coins can alter the OP_RETURN data field of each output. The respective outputs will still be worth one satoshi but it will also represent whatever the coloured coins issuer has decided it should represent. After some coloured coins have been issued, they can be traded just like any other bitcoins, the miners will not treat these transactions any differently. The redemption of coloured coins, i.e. the exchange for the underlying asset which the coloured coins are meant to represent, is the responsibility of the issuer and has nothing to do with the blockchain itself. The buyer of a coloured coin consequently needs to trust the issuer of the coloured coins in fulfilling his or hers promise on exchanging these coloured coins for the real-world asset it is said to represent.

Potential use cases using coloured coins include [36]:

- **Smart property** – The real-world asset represented by a specific coloured coin could be a property like a car or cell phone that can only be unlocked by the owner of a specific coin.
- **Company stock** – A stock certificate is typically digitalized already and should prove easier to implement as a coloured coin. A company could either issue new shares using the coloured coins protocol or it could move existing shares so that they are represented on the bitcoin blockchain instead.
- **Deterministic contracts** – Any financial derivative can be represented by a coloured coin.
- **Bonds** – Just like a company stock and a financial derivative, a bond is typically digitalized already and is by such a suitable coloured coin use case.
- Real world currencies or alternative digital currencies – A coloured coin could be said to represent 1 EUR or one new digital coin with an arbitrary name. Again, for a coloured coin to be worth 1 EUR, trust needs to put in the issuer of the coloured coin in regards to him or her exchanging real euros when requested by the holder of the coloured coin. In 2015, a project called Cuber, with an Estonian bank named LHV Bank as the core of the project, made a real-world experiment by issuing 100 000 EUR worth of coloured coins on the Bitcoin blockchain [37].

Some of the benefits with coloured coins include [36]:

- They are very general, practically any real world or digitized asset can be represented by a coloured coin
- They can be stored digitally without the need of a third party
- They can easily be traded between owners without the need of a third party
- They can be traded for other coloured coins or uncoloured coins in a single transaction, thus counterparty risk is removed

The reason for why the Bitcoin blockchain makes a good platform for coloured coins applications is that it is the most proven blockchain to date. On the other hand, the more general blockchain platform Ethereum [38] offers its users to create their own digital currencies. Thus, Ethereum can also be used to realize the concept of coloured coins. Some might even argue that it is preferable to use Ethereum for this purpose since the platform was built with the asset tokenization capability in mind whereas Bitcoin presumably was not.

4.2 Type of Blockchains

A blockchain can be either public or private and either permissioned and permissionless. The Bitcoin blockchain is public and permissionless and as such, has certain characteristics. As already pointed out, the use of blockchain has the potential to extend far beyond Bitcoin and cryptocurrencies. Many of the organizations and companies looking to adopt the blockchain technology experience issues [26], due to regulatory reasons or other [39], related to the public and permissionless structure inherent to Bitcoin. As a result, entities are increasingly interested in the private and/or permissioned types of blockchain since these might offer a solution more in line with their regulatory environment and current business models [40].

4.2.1 Public or Private

A public blockchain is a blockchain where anyone can read and submit transactions to the blockchain [41] [26]. Note that the phrase “submit transactions” refer to the ability to suggest transactions to the network. The question regarding who has permission to validate these transactions and subsequently put them in a block and attach it to the blockchain depends on whether the blockchain is permissioned or permissionless.
A private blockchain on the other hand is a blockchain where the permission to read and submit transactions is restricted to selected users [41][26]. To enforce the privacy of a private blockchain, all participants must identify themselves before entering the network meaning that the anonymity that may exist in public blockchains does not translate over to private blockchains. The lack of anonymity in private blockchains is an important aspect as it enables a blockchain of this kind to use a wider range of consensus schemes [42]. For example, a Sybil attack\(^2\) is not possible if blocks are created by a closed set of identified participants which means that the Proof of Work consensus algorithm used in Bitcoin is not needed in private blockchains [40].

If the identity of all network participants is known, legal contracts involving these identities can be established so that the rules of the blockchain are followed. If the rules are not followed, guilty participants can be identified. These participants must then absorb the consequences as described in the contract. The incentives for validators in a private network to follow the rules do not have to consist of a monetary reward as is the case with Bitcoin. The incentives will rather be to avoid legal penalties and of course, in the case where validators themselves benefit from a functioning blockchain network, to keep the network up and running.

A private network requires some type of Certificate Authority (CA) to issue identities and cryptographic certificates to nodes [43]. The CA is a trusted third party and as of such, the degree of decentralization is reduced in a private blockchain.

### 4.2.2 Permissioned or Permissionless

Whether a blockchain is permissioned or permissionless refers to which participants in the network that have permission to create new blocks that are to be propagated to the rest of the network [26]. Bitcoin relies on a permissionless blockchain meaning that all network participants can create new blocks given that some conditions are fulfilled [41]. In a permissioned blockchain however, nodes need prior authorization from a centralised authority in order act as a validator and block creator [41]. A permissioned blockchain can have one or several validators. If there is only one validator in a permissioned blockchain, no consensus mechanism is needed. A blockchain with only one validator, or miner as in the case of Bitcoin, does not carry the same degree of decentralization as a blockchain with many validators.

There is one key aspect that helps decentralize a network with as little as one validating node and that one refers to the fact that a copy of the blockchain is to be held at all nodes in the network. Even though the power to write new information to the blockchain is concentrated to only one participant or a few participants, all network participants can trace the history of events which makes it impossible for the “administrators” to alter data in the chain, without anyone noticing, because all participant has their own copy of the

---

\(^2\) A Sybil attack might appear when a node presents multiple identities and then uses these identities to control a substantial fraction of the system.
blockchain that suddenly would not match the new tampered version administrators might try to propagate to the network. When nodes in the network realize that the administrators are not validating blocks correctly, they will soon abandon the network and it will be rendered useless. This dynamic provides incentives for administrators to follow the rules.

A permissionless blockchain, to which anyone can connect and where participants’ true identities are not explicitly stated, needs to have a consensus algorithm that makes it expensive in monetary terms to attack the network. A permissioned blockchain on the other hand, in which the real-world identities of validating participants are known, can rely on a consensus algorithm that is reputation based in the sense that malicious behaviour is penalized through legal contracts or exclusion from the network.

4.3 Digital signatures

The concept of digital signatures is a crucial part of the Bitcoin protocol and presumably also in many future blockchain applications. With the help of public-key infrastructure, the network participants can verify that a transaction from one public address to another is valid because the owner of the sender’s address has signed the transaction using its private key [32]. Each address in the network is a public key [44] and each public key has a corresponding private key to which it is mathematically connected. In Bitcoin, a user can create as many addresses as it wants [33] [4]. Each address is characterized by a public/private key pair. If the sender’s public key matches the sender’s private key in a transaction, we can be sure that the one initiating the transfer of coins owns the referenced UTXOs. This mechanism ensures that no one in the Bitcoin network can spend someone else’s coins unless the private key is stolen. Digital signatures provide a strong control of ownership but it does not prevent double-spending, that is rather the purpose of the Proof of Work consensus algorithm. [1]

4.4 Consensus algorithms

In a decentralized database powered by a blockchain, there needs to be a consensus mechanism so that participants can agree on the current state of the blockchain. In technical terms, consensus in a blockchain network means that the nodes have agreed on one single version of the blockchain and thus there are no separate branches of the chain. In a traditional system, trust is simply put in the centralized authority in respect to providing the true state of the database. When it comes to payments, banks often act as the centralized authority. The bank executes different transactions and we trust that it does so in a correct manner. However, if a decentralized and trustless system where no intermediaries is desired, the network participants needs to agree on the current on their own. The participants in a blockchain network can do so using a consensus algorithm that essentially enables the nodes to vote for what they think is the correct state of the blockchain database.

A trivial consensus algorithm would let nodes cast votes, in an effortless manner, on the version of the blockchain they think is correct. However, due to the threat of a Sybil
attack, such an algorithm cannot be trusted to achieve consensus just like most online polls cannot be trusted to contain votes from only unique individuals [42]. To avoid the threat of a Sybil attack, Bitcoin uses an algorithm called Proof of Work where one unit of computing power is equivalent to one vote [45]. The approach of one unit computing power representing one vote makes it expensive to gain a disproportionate share of control in the system. Proof of Work and other consensus algorithms is described in the next section. All consensus algorithms described in this thesis share a principle called the longest valid chain principle.

The longest valid chain principle means that nodes will accept the longest chain as the correct version of the blockchain [44]. All honest nodes in the network keeps working on creating the next block in the longest chain. The scenario of an adversary trying to double-spend its bitcoins is a good example of how the longest valid chain principle work. Figure 9 illustrates a chain of blocks in which a transaction, where a consumer A pays a merchant B one Bitcoin for a product, has been accepted in to the latest block of the blockchain. The new blockchain is immediately propagated to the rest of the network and all nodes subsequently has a copy of the same blockchain. At this point, there is consensus about the true state of the blockchain. Merchant B sees that the transaction has made it into the blockchain and consequently initiate the shipping of product to consumer A.

![Figure 9. A transaction makes it into a block](image)

Consumer A gets a confirmation that the product has been shipped and a successful transaction has ultimately been made. However, consumer A is going to try to make the block containing its transaction invalid by creating another block that refers to the preceding block rather than the newly created block. This is an attempt on the part of consumer A to double-spend its money by creating a new branch in the hope of making it the longest chain. In the block, consumer A includes a transaction to itself. Consumer A propagates its newly mined block, which is illustrated in Figure 10, to the rest of the network.
“A” tries to double-spend its bitcoin by creating a new longest chain, thus making the original one invalid.

The network will acknowledge that there now are two blocks referring to the same preceding block. A so-called fork has appeared. The concept of forks is important and is described more in detail in section 4.6. Nevertheless, nodes will continue to reference the “A to B” block when trying to create a new block because that was the block that was first received. This decision to keep on working on extending the chain that became longest first is a matter of following the Bitcoin protocol but in the eyes of the network, both blocks are equally correct, it is just that the “A to B” block arrived first. For A to successfully double-spend its money, in the sense that it gets to both keep its bitcoin and get the product, it needs to create the next block and attach it to the “A to A” block before another block is attached to the “A to B” block. If A is successful in doing so, it will propagate this new version of the blockchain to the rest of the network and since it is now the sole longest chain, nodes will accept this version as the correct one, and thus start working on prolonging this new branch, and the double-spend attack is ultimately successful. Figure 11 shows how the original branch becomes invalid.

“A” is successful in creating a new longest chain, hence the double-spend attempt is successful. A gets the product while keeping its bitcoin.

The ability for consumer A to be able to create a new block before the rest of the network is heavily restricted by the consensus algorithm. A node cannot just create a block at will, hence why the term “trying” was used when the adversary was to prolong its chain. First,
a node needs to prove that it has the right to create the next block. In general, to avoid the opportunities to double-spend, a good consensus algorithm makes it unlikely that one node gets to create two or more blocks in a row. In a blockchain where it is very unlikely, or impossible, to create two blocks in a row, a much more realistic scenario would be that the rest of the network creates the next block and hence prevent the double-spend attack. Figure 12 illustrates the more likely scenario of another block being built on top of the original chain.

Consumer A does not need to give up its double-spend attempt at this point. It can keep on trying to create blocks and attach them to its chain and nodes in the network will keep on acknowledging them as part of an invalid branch unless it outpaces the other branch and becomes longer. As already implied, the chance of this happening is very low in a functioning blockchain network. In fact, in the case of Bitcoin, the probability of A’s branch becoming longer decreases exponentially as the lead in the number of blocks increases [1]. As a consequence, merchant B can feel more and more secure that the transaction is irreversible as more and more blocks are added on top of the block containing that particular transaction.

Figure 13 shows how forks appears at two points. The figure does not tell whether the invalid branches were part of the longest chain at some point, it merely shows that these branches were discarded meaning they did not make it in to the blockchain in the long run. If a branch of blocks is not part of the one true blockchain, and no node is working on extending that branch, the blocks in the branch is referred to as “orphaned blocks”.

Figure 12. “A” is unsuccessful in its attempt to double-spend its bitcoin
It is important at this point to emphasize that forks can appear without a node trying to perform a double-spend attack [4]. In a large network like Bitcoin, honest nodes might try to propagate new blocks at the same time. Some nodes might think that a certain block arrived first and start working on extending that block while others might think that another block arrived first and start working on extending that instead. An identical race to the one in the double-spend attack scenario unfolds. Again, the branch that first becomes the longest will make it into the one true blockchain. So regardless if a merchant believes that a double-spend attack might be attempted, it can be advisable to wait until the relevant transaction has been buried under an arbitrary number of blocks. Bitcoin mitigate the risk of forks appearing by having a build in mechanism that makes sure that a block is created every 10 minutes on average. Sometimes a node is able to generate a block in a shorter time frame and sometimes it takes longer. By spreading out the probable time for which a new block is created, the risk of nodes proposing new blocks at the same time, and thus create forks, is reduced. In general, a sound blockchain protocol has a low probability of multiple nodes creating new blocks at the same time [26].

4.4.1 Proof of Work

Proof of Work is the inherent consensus algorithm used in the majority of currently existing digital currencies [46], with the leading cryptocurrency Bitcoin leading the way [1]. Proof of Work is essentially about nodes having to solve a computationally intense puzzle to be able to create the next block in the blockchain. In the case of Bitcoin, a node that is successful in solving this puzzle, and hence get to create a new block in the blockchain, is rewarded bitcoins. This reward coupled with the transaction fees described briefly in section 4.1.2 is what incentivise nodes to create new blocks. New bitcoins are consequently created for each new block and that is why the Proof of Work procedure is called “mining”.

The procedure of creating a new block in the Bitcoin network goes as follows. First, for the block to bear any significance there needs to be some data in it. In the case of Bitcoin, blocks are filled with transactions that users in the network has initiated. For the transactions to be completed in the sense that bitcoins change ownership, the miner first needs to validate that the transactions are correct and then it must “solve” the computationally intense puzzle. The solution to the puzzle is called Proof of Work. Every valid block in the blockchain contains a Proof of Work.
The miner validates transactions by checking that the sender of each transaction has signed the transaction using his or her digital signature and that this signature matches the public key in possession of the referenced UTXOs. Furthermore, a check whether the sender in fact has the required funds to carry out the intended transaction is made. When the transactions have been validated, one thing remains and that is to produce the Proof of Work. *Now the miner needs to use its computing power to make sure that the hash of the block is below a given threshold.* Since all variables except one in the block is already set (the transactions, the timestamp, the pointer to the preceding block’s hash), the variable that needs to be manipulated to find an acceptable hash is the nonce. The miner tries to find an acceptable hash by constantly incrementing the nonce until the hash of the block finally is below the given threshold. When this is done, the miner proposes to the rest of the network that the newly mined block is included in the blockchain. If all the transactions have been validated correctly and the block hash fulfills the requirement, the block will be accepted by all the nodes and the miner can reap its reward.

Satoshi Nakamoto [1] summarizes the steps needed to run the Bitcoin network:

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult Proof of Work for its block.
4. When a node finds a Proof of Work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

When discussing the Proof of Work algorithm, it is instructive to relate it to the longest branch principle previously discussed. The longest branch principle in Proof of Work means that the correct version of the blockchain is the chain to which miners have sacrificed the most work in terms of computing power [1] [4]. Since each block is required to contain a Proof of Work, a completed block can be seen as one unit of work. Consequently, the longest chain of blocks contains the most amount of work.

Note that Proof of Work needs to be combined with some kind of reward to offset the electricity and hardware cost associated with the computations required to find a valid hash for a specific block. As already mentioned, Bitcoin does this by rewarding its miners with bitcoins for every block they create.

### 4.4.2 Proof of Stake

Proof of Stake algorithms use another method for deciding who gets to create the next block. Instead of letting nodes use vast amounts of computing power to solve the computationally intense puzzle inherent to cryptocurrencies like Bitcoin, Proof of Stake selects the next block creator in a deterministic pseudo-random way [47]. The probability of a node getting to create the next block is proportional to the amount of stake that node has in the blockchain network [5]. In the case of cryptocurrencies, the amount of stake
could be equivalent to the amount of wealth relative to the total outstanding currency balance [47].

For other applications than cryptocurrencies, one would have to find another quantitative asset that represent the stake held in the network. The logic behind the Proof of Stake is that nodes that hold stakes in the network have incentives to validate transactions and create blocks correctly because if they do not, their stake will be damaged.

A block creator in the Bitcoin network is called a miner. It is unclear if this terminology will extend to other applications than cryptocurrencies if Proof of Work is used. When Proof of Stake is used in cryptocurrencies, a block creator is commonly referred to as a “forger”. [47]

4.4.3 Mining diversity

MultiChain [48] is a blockchain platform with a focus on private blockchains. MultiChain uses a consensus algorithm called “Mining diversity” which lets network participants take turn validating blocks in a round-robin order. Since all participants in a private network is backed by their real-world identities, a permissioned blockchain does not have to worry about Sybil attacks [45]. The Mining diversity algorithm can specify that a node only has permission to mine a block if a predetermined number of blocks have passed since the last block it mined. The implication of this approach, given that the mining diversity parameter is not set too low, is that no node can mine two blocks in a row thus making it impossible to double-spend unless a node successfully colludes with another node.

4.5 51% attack

A 51% attack is one of the most serious attack on a blockchain [22]. Many consider a “real” blockchain to be immutable in the sense that once a record makes it onto the blockchain, there is no way to change it or delete it. That is not the case under all circumstances. In theory, as briefly discussed in section 4.1.2, an adversary wishing to tamper with past records in the Bitcoin network can do so by controlling 51% of the computing power [45].

A node controlling 51% of the network will create 51% of all new blocks and will, eventually, be able to outpace any competing branch of the blockchain. If an adversary wishes to tamper with a block deep in the blockchain, and it “only” controls 51% of the network, it might take a long time for that the adversary’s branch to become the longest branch because 49 of every 100 blocks created will work on prolonging the original longest branch (on average). Nonetheless, eventually the adversary will have caught up and succeeded in creating the longest branch and hence, the nodes will consider this new chain to be the true state of the blockchain. All transactions included in the original blockchain will be rendered invalid and the adversary would have been effective in its objective of tampering with the blockchain.
In general, the more expensive it is to control 51% of the network, the more secure the blockchain is [22]. In the case of Bitcoin, the cost of acquiring 51% of the network’s computing power is quite substantial. The motivations behind why someone would might want to launch a 51% attack are several. One motivation could be that the adversary is trying to double-spend its money. Another motivation could be the wish to censor transactions related to certain parties and a third could simply be the will to sabotage due to the adversary having interests in the failure of the network. If the objective is to create a permissionless blockchain or a permissioned blockchain with several validating nodes, it is of the outmost importance from a security perspective to make sure that no single person or group can launch a 51% attack.

The risk of a 51% attack is generally higher the smaller the network. This is not as much of a problem in the case of a private network in which all participants are identified by their physical identity, as is the situation in all use cases identified in this thesis. If participants in a private network decided to collude in an attempt to alter the blockchain to their advantage, it will be easy for the rest of the network to identify these participants. For colluding participants to be held accountable for their crimes, it is very important to have legal documents stating acceptable and forbidden behaviours in the network.

4.6 Forks

The Bitcoin protocol states that each miner should keep on building on the longest branch of blocks [1]. A blockchain fork can appear when the network does not agree on which branch of blocks is the longest [49]. One very important feature of a blockchain is that nodes should agree on one single transaction history and thus, forks are unwanted because they essentially represent two different and conflicting versions of the blockchain. A fork can typically appear when two miners propagate new blocks to the network at nearly the same time [50] but they can also happen as part of an attack [51].

An attack could be in the form of a double-spend attack or just an arbitrary attack with the purpose of destabilizing the blockchain. A fork in technical terms means that there are two different blocks that refers to the same preceding block. Miners must decide on which of these two blocks they are going to refer to when creating the next block and they make this decision based on which block they were made aware of first. Due to propagation latency, some nodes will think that one block arrived before the other and some nodes will think the opposite meaning that a fork has become a fact.

A fork is commonly solved using a blockchain’s consensus mechanism. In the case of Bitcoin, miners will continue to try extending the latest block in, what they think, is the longest branch. When a fork appears, there will be a sort of race between the two different branches held by two groups of miners in the network in terms of which one is extended first. The branch that is extended first becomes the longest chain. All nodes working on the branch that lost the race must accept defeat and accept the other chain as the correct one which means that they will try to extend that branch rather than the one they previously worked on. It is very unlikely, in a properly designed blockchain, but not
impossible, that the race renders a draw meaning that the two competing mining groups succeeds in mining a new block at approximately the same time, again. In that case, the race effectively continues and the fork will most likely be resolved when the next block is mined, making one of the competing branches the longest chain. A sound blockchain protocol mitigates the possibility of two blocks being created at the same time [26].

4.7 Blockchain versus a conventional centralized database

Gideon Greenspan argues [8] that if trust and robustness are not an issue, there is nothing a blockchain can do that a regular database cannot. In the cases where blockchain is preferable, the ambition to use this technology is driven by cost. Greenspan describes the respective advantages as follows:

Blockchain advantages:

- Disintermediation
- Robustness

Conventional centralized databases advantages:

- Confidentiality
- Performance

Regarding *disintermediation*, this is where a blockchain can offer something new that a conventional database cannot. A blockchain enables data to be shared across a network on a peer-to-peer basis without the need of a centralized administrator that facilitates the transaction. It is the consensus mechanism in a blockchain that essentially removes the need for a centralized facilitator, the so-called middleman, in the network. The reasons for why one would want to get rid of the middleman may not be obvious. There are many examples of functioning systems that uses intermediaries. When sending money to another person’s bank account, the bank work as an intermediary and they always, to the best of our knowledge, does this correctly. When buying stocks at an online broker, there are several intermediaries making sure that the ownership stocks changes hands and that the person that should to get paid, is paid [52]. The reason why we would want to get rid of these intermediaries is not because they do not work. It is because they work in an inefficient, time consuming and costly manner. The blockchain at its core replaces these intermediaries with code so that two parties wanting to do business with each other can do so as quickly and cheaply as possible.

The next advantage in a blockchain-powered database is *robustness*. A conventional centralized database is vulnerable to attacks on the centralized node on which the database is run. In a blockchain network there is no single point of failure since the data is redundant on all the nodes on the network. There are of course mechanisms build in the centralized database to make sure that a loss of power, or some other problem at the
centralized node, does not make the whole system fail. These mechanisms include backups that takes over in the event of failure in the primary server. However, this type of solution is both expensive and hard to configure. A blockchain network is an efficient way to maximize a database’s robustness as it will not get compromised unless a majority of nodes are compromised.

If confidentiality is important, it is advisable to use a centralized database over a blockchain. This has to do with the fact that all nodes that validates transactions over the blockchain needs to be aware of all previous transactions. On the other hand, a sole trusted intermediary can keep all transactions secret between participants in the network.

When performance is considered, a centralized database is preferred over a blockchain-powered database [42]. Except for the actions a centralized database needs to perform, the blockchain needs to do three additional things. These are:

- Signature verification. Unlike in a client-server network, in a peer-to-peer network such as a blockchain network, transactions that are send between nodes needs to check for its origin. If we consider one transaction in the Bitcoin network, one needs to be sure that the sending side of the transaction in fact has initiated the transaction. This is done by checking the digital signature of the transaction.
- Consensus mechanism. There are different consensus algorithms, some more burdensome that others. In any case, a blockchain peer-to-peer network requires nodes to communicate back and forth to reach consensus on the true state of the database. In a client-server model, the server simply provides the true state always.
- Redundancy. For every transaction in the network, each node needs to process it. In a centralized database, each transaction is only processed once.

### 4.7.1 Blockchain versus a distributed database

A blockchain is a type of distributed database in the sense that the data is replicated over several nodes [41] but there are some differences relative to a conventional distributed database. A distributed database is “a collection of multiple, logically interrelated databases distributed over a computer network“ [53]. A distributed database is constructed in such a way that information is spread out on several databases with the purpose of retrieving and processing information faster [41]. A common set up for distributed databases is the so called primary-secondary architecture which is logically centralized with one database (the primary) controlling all the secondary databases [54]. All updates to the database must go through the primary database. Another architecture, which properties are more similar to a blockchain’s, is called multimaster replication in which all nodes can write to the database. Any change to the database is replicated to all other nodes without the change having to go through one specific database. Multimaster replication is advantageous relative to the primary-secondary architecture since the former has no single point of failure whereas the latter has one at the primary node. The
set of connections through which data is replicated to all the nodes is called the replication topology [55].

The difference between a distributed database with multimaster replication and a blockchain is that the distributed database depends on nodes trusting each other. In a distributed database of this kind, nodes trust the data that is being transmitted to them through the replication topology. If one node starts to display malicious behaviour by relaying corrupt data to other nodes, the database will start to become inconsistent. This problem of nodes having difficulties reaching consensus on the system state due to a potential malicious node existing in the network is called the Byzantine General’s Problem [56].

Richard Gendal Brown illustrates the main difference, which is the dependence on trust among nodes, between a distributed database (Figure 14) and a distributed ledger (Figure 15). [30]

![Figure 14. Distributed database](image1)

![Figure 15. Distributed ledger](image2)
Consensus algorithms have been developed, before the emergence of blockchain, to combat the Byzantine General’s Problem within conventional distributed. These algorithms are called Byzantine Fault Tolerant (BFT) consensus. A distributed database incorporating BFT consensus needs to know the identity of all nodes in the network which is also true for a permissioned blockchain, while a permissionless blockchain does not have this requirement. Another difference is the respective technologies ability to scale [43]. While a distributed database using BFT consensus has better performance in terms of the number of transactions it can process per second, a blockchain has better scaling properties when it comes to the number of validating nodes in the network.

In conclusion; the cryptographic linking between blocks, coupled with a consensus algorithm such as Proof of Work, enables a blockchain to overcome Byzantine failures and ultimately come to a global agreement of the current state of the database. A blockchain can reach this consensus relatively easy whereas the consensus processes available in decentralized distributed database involves a lot of messages back and forth which makes it difficult to scale the number of nodes [43].

4.8 Smart contracts

The term “smart contract” is said to have been popularized by computer scientist Nick Szabo in a 1994 essay. In the essay, Szabo describes a smart contract that enforces car loan payments by prohibiting the owner of the car to access it in the event of him or her failing to deliver loan payments in a timely manner. The restricted access would be carried out programmatically and automatically. [57]

In essence, a smart contract is a piece of computer code that enforces a contract automatically given some event occurring, or not occurring as in Szabo’s example, in either the physical or digital world. From this concise definition, one can conclude that a smart contract does not necessarily need to exist on a blockchain. However, it does make sense to combine the idea of smart contracts and blockchains. Contracts have traditionally needed middlemen to enforce them. As already described, blockchains are mainly about disintermediation. In the case of Bitcoin, it is the disintermediation of value transfer. Using smart contracts, the process of enforcing contracts also has the potential of being disintermediated, thus making the contracting process more efficient.

Smart contracts are scripts that are stored on the blockchain. These contracts have unique addresses to which nodes can send transactions. When a contract is called upon by a transaction, its code is triggered and a deterministic action is performed independently by all nodes in the network. The action that is performed reads or write new data to the blockchain according to the smart contract code [42] [58]. Since every node in the network will run a particular smart contract independently, it is essential that the smart contract is deterministic in terms of it producing the same output for every identical input. If a smart contract would fail in delivering the same output for all nodes, the blockchain would become inconsistent and a permanently inconsistent blockchain among honest
nodes is, if not simply useless [58], no longer a single blockchain, but rather several different ones.

Richard Gendal Brown, from which the definition of Distributed Ledger Technology was drawn earlier, has also articulated a smart contract definition [59].

*A smart-contract is an event-driven program, with state, which runs on a replicated, shared ledger and which can take custody over assets on that ledger.*

A crowdfunding project is a good example of a simple but useful smart contract application. Commonly, for a crowdfunding project to be successful, it must raise a certain amount of money. If the entrepreneur seeking funds for a project only gets half what is needed to complete the project, the crowdfunding has failed and money should go back to the people that tried to fund the project. Typically, there exists a centralized entity that collects and distribute the money. A smart contract enabled blockchain could help decentralize the act of crowdfunding by having a smart contract collecting all the money and, if the total funds received amounts to the target, or exceeds it, the contract then pays the entrepreneur. In contrast, if not enough money was received by the contract to reach the goal, the contract would simply pay back the money to its respective originating addresses. Since the smart contract resides on the blockchain, which every node in the network holds a copy of, nodes can easily inspect the contract and make sure that the code executes as expected.

5. Results

The results section of this thesis consists of several identified blockchain use cases related to Scania. A critical analysis of each use case has been made using the analysis model as described in section 3.1.

5.1 ScaniaWallet

ScaniaWallet refers to the idea of using a coloured coin protocol to leverage an existing blockchain, such as Bitcoin’s or Ethereum’s blockchains, to issue a digital currency called ScaniaCoin. The ScaniaWallet could enable Scania customers, i.e. the hauliers, to use ScaniaCoins to transact with agents such as repair shops, towing companies and fuel stations. Potential benefits include:

- Lower total transaction costs from the perspective of the ecosystem as a whole (Scania, Scania’s customers and agents as a collective)
- From the perspective of agents, credit risk is shifted from individual customers to Scania, who is presumably more creditworthy
- Payments are performed in near real-time
The background for ScaniaWallet consists of three parts. First, in today’s conventional payment system, agents typically pay a floating fee [60] to a financial payment card company such as VISA for every transaction received. The initial hypothesis is that the cost of using ScaniaCoins will be lower than the costs associated with payment systems used today. The second part of why ScaniaWallet is interesting relates to the perceived creditworthiness of Scania’s customers, i.e. the hauliers, from the perspective of agents. Small hauliers may run the risk of being denied service from agents due to agents’ concern regarding hauliers’ ability to pay for their services. The hypothesis related to this issue is that agents would have more faith in ScaniaCoin and their ability to exchange this currency for a fiat currency, the consequence of which would be that small hauliers could enjoy the credit worthiness of Scania and, as a result, avoid denial of service from agents. Finally, a blockchain system has the potential to process payments faster than conventional payment processors meaning that small, foreign hauliers that is required to pay cash does not have to wait too long for their payment to settle before receiving service by agents.

These three hypotheses can be summarized as follows:

1) The costs of using ScaniaWallet is lower compared to the costs associated with the current conventional payment system between hauliers and agents where transactions need banks and payment processing companies to act as intermediaries.
2) The benefits of using ScaniaWallet to increase hauliers’ creditworthiness outweighs any potential disadvantages related to the shift in credit risk.
3) ScaniaWallet enables faster payments through near real-time settlement on the blockchain. The difference in settlement time is especially large if payments occur on weekends or holidays.

For the ScaniaWallet use case to be considered useful, at least one of these hypotheses must hold true. To investigate these hypotheses, and the relevance of the use case in general, it is useful to make a comparison between the current payment system and ScaniaWallet, both with and without the use of blockchain technology. Figure 16 illustrates the current payment system where hauliers pay agents using conventional intermediaries such as banks and payment processors. The transaction fee associated with this transaction is denoted TF1 and is typically carried by the merchant (agent) [61].
Next, ScaniaWallet without the use of blockchain technology, from now on referred to as the centralized ScaniaWallet, is considered in Figure 17. Here, Scania essentially acts as a bank between a haulier and an agent. This approach resembles the conventional payment system illustrated in Figure 16 but with a few additional required steps to close the ecosystem.
The steps in Figure 17 are denoted using numbers 1 to 5 and have the following meaning:

1) The haulier transfers money to Scania in exchange for ScaniaCoins. This transaction is made using a bank and is associated with a fee denoted TF2a. Scania updates its central servers so that the haulier’s account now has a number of ScaniaCoins equivalent to the value of the bank transaction.

2) The haulier wishes to transact with an agent. A signal with information about the transaction, i.e. how many ScaniaCoins that are to be deducted from the haulier’s account, is send to Scania’s central servers.

3) Scania updates its database by deducting funds from the haulier’s account while at the same time increasing the equivalent amount of funds in the agent’s account.

4) At some point, the agent will want to exchange its ScaniaCoins in return for a predetermined fiat currency. The agent sends a message to Scania detailing how many ScaniaCoins it wishes to exchange.

5) Scania exchanges the ScaniaCoins by returning an amount according to a predetermined exchange rate. This transaction is made using a bank and is associated with a fee denoted TF2b.

ScaniaWallet without a blockchain solution is a centralized system where all communication must go through Scania. The implications of such a system will be discussed in the analysis part of this use case. Concerning hypothesis 1, we can now formulate an equation that must hold true in order for the hypothesis to hold true. This equation can be formulated as

$$TF2a + TF2b < TF1$$  \hspace{1cm} (1)

The sum of TF2a and TF2b, the transactions associated with the centralized ScaniaWallet, must be lower than TF1, the transaction fee associated with the conventional payment system, for hypothesis 1 to be true. To finish the comparison, ScaniaWallet using blockchain technology, from here on referred to as the decentralized ScaniaWallet, is considered in Figure 18.
Figure 18. Decentralized ScaniaWallet using blockchain technology. A total of five different transactions fees are associated with this system.

The steps in Figure 18 are also denoted using numbers 1 to 5. Step 1 and 5 is almost identical to the corresponding steps in the centralized ScaniaWallet system while steps 2, 3 and 4 differs. The numbers now have the following meaning:

1) The haulier transfers money to Scania in exchange for ScaniaCoins. This transaction is made using a bank and is associated with a fee denoted TF3a.

2) Instead of updating its central database, Scania instead issues the right number of coloured coins; ScaniaCoins, and sends them to the haulier’s blockchain address. This transaction must be verified by the miners of the blockchain and is therefore associated with a fee. This fee is denoted TF3c.

3) The haulier can now make a decentralized transaction by paying an agent over the blockchain network in a peer-to-peer fashion. Again, this fee is associated with a transaction fee attributed to the miners. This fee is denoted TF3d and will be of approximately the same size as TF3c.

4) At some point, the agent will want to exchange its ScaniaCoins in return for a predetermined fiat currency. The agent exchanges its ScaniaCoins by sending its ScaniaCoins to Scania’s blockchain address. Just like step 2 and 3, this transaction goes over the blockchain, thus a fee is incurred. This fee is denoted TF3e and will be approximately the same size as TF3c and TF3d.

5) Scania exchanges the ScaniaCoins by returning an amount according to a predetermined exchange rate. This transaction is made using a bank and is associated with a fee denoted TF3b.

Just like for the centralized ScaniaWallet, an equation can be formulated regarding hypothesis 1, but this time in relation to the decentralized ScaniaWallet. The equation that
needs to hold true for hypothesis 1 to hold true, in the case of the decentralized ScaniaWallet, is

\[ TF3a + TF3b + TF3c + TF3d + TF3e < TF1 \]  \hspace{1cm} (2)

The assumption that all transactions over the blockchain network will have approximately the same fee can be formalized in the following equation

\[ TF3c \approx TF3d \approx TF3e \]  \hspace{1cm} (3)

Furthermore, since step 1 and 5 is identical for the centralized and decentralized ScaniaWallet, the transactions corresponding to these steps and their relationship can be formulated as

\[ TF2a = TF3a \] \hspace{1cm} (4)
\[ TF2b = TF3b \] \hspace{1cm} (5)

Using equations 1, 2, 4 and 5, the following relationship must hold if one assumes that transaction fees over the blockchain is free, i.e. the cost is for these transactions are 0 (TF3c = TF3d = TF3e = 0)

\[ \sum_{TSs} TFs \text{ decentralized SW} = \sum_{TSs} TFs \text{ cecentralized SW} \] \hspace{1cm} (6)

If transaction fees over the blockchain is not free, as is the case in Bitcoin at the time of writing, then the following relationship must hold

\[ \sum_{TSs} TFs \text{ decentralized SW} > \sum_{TSs} TFs \text{ cecentralized SW} \] \hspace{1cm} (7)

From equation 6 and 7, one can conclude that the decentralized ScaniaWallet carries the same amount of transaction fees as the centralized ScaniaWallet if transactions over the blockchain are free whereas it is more expensive relative to the centralized ScaniaWallet in the case of blockchain transactions not being free. Note that the cost of servers that is associated with running a centralized ScaniaWallet is neglected. Also, the transaction cost for Scania to acquire bitcoins, which are meant to be coloured and issued as ScaniaCoins, in the case of the decentralized ScaniaWallet, is ignored as this cost is considered an investment cost, as opposed to an operating cost, to get the system up and running.

5.1.1 Analysis

Complexity

The complexity related to implementing the currency part of a decentralized ScaniaWallet is relatively low as there are several existing vendors offering a way to implement a digital currency using blockchain technology. Therefore, the technological aspects inherent to this use case will not likely be a bottleneck. What might prove more difficult could be to
grow the network to a satisfactory extent so that participants can use ScaniaCoins as a mean of payment at enough places for the network to become valuable for them. Just like most networks, the ScaniaWallet network will become more valuable the more users are in it and since this type of use case, in which a company issues its own currency that is meant to be used externally, seems to be untested on a large scale, agents and hauliers might hesitate to join the network, thus creating a “chicken or the egg” dilemma.

The complexity of implementing the centralized ScaniaWallet is even lower as it only requires Scania to run a database that keeps track of all the balances of ScaniaCoins in the network.

Even though this thesis set out not to discuss the legal aspects of the proposed use cases, this aspect should at least be briefly mentioned when discussing complexity. This is because payments of this kind are likely to be heavily regulated by financial authorities. Given that the technological implementation, in terms of issuing the currency, and the scaling, in terms of getting enough participants in the network, is successful, the legal aspect is likely to bear the highest complexity.

**Value proposition**

The value for Scania related to this use case is higher customer satisfaction due to them being able to enjoy the credit worthiness of Scania when dealing with agents. Hauliers that experiences denial of service due to perceived low credit worthiness by agents will have another incentive to choose Scania as a supplier since ScaniaWallet offers a solution to this problem. Of course, credit risk does not disappear with the use of ScaniaWallet. The credit risk that agents had to bear when selling services to hauliers is now absorbed by Scania. Such a shift in the bearer of credit risk is only directly beneficial if Scania has a better ability to claim the credits that are given to hauliers. Whether such an ability exists is not known by the author of this thesis but what Scania might suffer in credit losses could perhaps be compensated by a higher number of trucks sold given that hauliers value this kind of service.

ScaniaWallet has another potential benefit and it has to do with a blockchain’s potential ability to settle payments faster than conventional payment systems. Even in the cases where hauliers have the will and ability to pay agents in cash, it takes a while for the money to show up in the receiving agent’s account. If the agent has no prior relationship with the haulier in question, the agent might hold the vehicle until it can see that the money has been received. Depending on when the service is delivered (after office hours, weekends), the time to settle a payment using the conventional system can vary from a few hours to a few days. On the other hand, a Bitcoin payment is considered to be settled in approximately 60 minutes meaning that the issue of hauliers having to wait to get their truck back on the roads due to payment latency is mitigated.

Neither Scania nor the hauliers is assumed to carry any direct transaction costs in the current payment system so the potential of lower transaction costs that ScaniaWallet
might offer does not affect Scania directly. In fact, TF3a and TF3b means that both the haulier and Scania would have to accept a transaction fee respectively, if using the decentralized ScaniaWallet, whereas the current system does not pose any transaction fees at all for these parties. Instead, the current system receives it transaction fees from the agent involved (TF1). Table 1 summarizes the shift in transaction fees. It is assumed that only the sender of a bank transaction between companies (TF3a, TF3b) pays a transaction fee. The transaction fees marked in bold is associated with transactions over the blockchain.

Table 1. Comparison of transaction fees

<table>
<thead>
<tr>
<th></th>
<th>Current payment system</th>
<th>Decentralized ScaniaWallet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agents</td>
<td>TF1</td>
<td>TF3e</td>
</tr>
<tr>
<td>Scania</td>
<td></td>
<td>TF3b, TF3c</td>
</tr>
<tr>
<td>Hauliers</td>
<td></td>
<td>TF3a, TF3d</td>
</tr>
</tbody>
</table>

Given Table 1 above, it is clear that TF3e needs to be less than TF1 in order for agents to have a direct economic incentive to join the network. Whether this is the case is not obvious since both TF1 and TF3e can vary. For ScaniaWallet to be feasible, all participants need to have an incentive to take part in the network. While Scania’s incentive is to provide a better service for its customers, i.e. the hauliers, and the hauliers incentive is to receive this improved service, it is not obvious what the incentive for agents would be if not lower costs. Nonetheless, if transaction cost does not become lower using ScaniaWallet, some other incentive needs to be introduced on the behalf of agents.

**Corresponding centralized solution**

The difference between the centralized and decentralized ScaniaWallet lies in, not surprisingly, the degree of decentralization. Even though both approaches rely on Scania exchanging ScaniaCoins and fiat currencies, the decentralized ScaniaWallet has all its transactions going through a blockchain network and thus, has a higher degree of decentralization. Equation 6 and 7 shows that the decentralized ScaniaWallet will carry the same amount of transaction fees as the centralized ScaniaWallet, if transactions over the blockchain are free; and it will carry higher transaction fees, if transaction over the blockchain are not free. In conclusion, the potential extra transaction fees inherent to the decentralized ScaniaWallet is a cost inherent to having the transactions being processed and validated by a pool of miners rather than Scania alone. The benefit, from the point of network participants, would be that less trust needs to be put in Scania in terms of processing payments and keeping track of ScaniaCoins ownerships. Trust would instead
have to be put in the blockchain network. Still, participants would have to trust Scania in regards to exchanging their ScaniaCoins for the pre-agreed fiat currency.

5.2 Platooning

The activity of two or more trucks driving in the same direction in close proximity to each other is called platooning. The distance between the trucks can be optimized to reduce the air drag that acts on the truck. The main benefits of platooning include reduced fuel consumption and, consequently, reduced carbon dioxide emissions and lower fuel costs for hauliers. However, the advantages enjoyed by the fleet of trucks platooning, as a collective, is not distributed evenly among participants. The truck that drives first in the platoon will not benefit, nor will it suffer to be fair, by participating in the platoon. Furthermore, the benefits between subsequent trucks, i.e. the trucks following the leader truck, in the case of a platoon with three or more trucks in it, are also not evenly distributed.

In the case of a platoon with trucks that are from the same haulier, the uneven distribution of cost savings among trucks is a non-issue as the haulier owning all the trucks in the platoon will absorb the total cost and hence, also the total benefits of the platoon. To push different hauliers, with perhaps different truck brands in their fleets, to embrace the act of platooning together, a system which keeps track of how much each haulier has contributed to the platooning community’s overall cost savings might help. Such a system could decide the order of trucks in a planned platoon so that a truck that has acted as the leading truck in a previous platoon has a greater chance to be placed further back in the next platoon. The idea is that all hauliers in the platooning community will be able to share platooning benefits evenly over time. Also, if hauliers wish to settle differences in benefits directly after a platooning event, the system could arrange transactions so that the platooning leader is paid by the other participants in relation to how much fuel cost that has been saved collectively. Immediate settling would ensure that the benefits acquired by platooning is shared among participants as soon as the platooning activity ends.

A system that keeps track on the positions of each truck in a platoon can be implemented using both a centralized approach and a decentralized, blockchain based, approach. Again, for the sake of comparison, both approaches are considered.

A centralized approach could be implemented by letting trucks in the platoon send positioning data to a central server held by Scania. If other truck brands other than Scania are to be included in the system, a joint ownership of a central database, between Scania and the brands in question, would be desirable. In either case, the positioning computations, with the purpose of deciding the order of trucks in the platoon, would be made centrally at this server. When planning for a new platoon, the system would allow participants to form platooning groups. Given a platooning group, the system would then compute the optimal order of trucks. The optimal order refers to the order that evens out previous platooning cost benefits among participants to the greatest extent possible. The
order would therefore depend on the historical platooning data of each participant. The haulier in the platooning group who has enjoyed the most fuel savings thanks to the platooning network would presumably have its truck placed first in the order of trucks.

The main challenge with a centralized system of this sort would likely be the operation and maintenance of the shared centralized database. Participating hauliers in the platooning system would need to trust the entity keeping track of historical positions. Furthermore, the centralized entity would need to be compensated for its work, thus creating a cost to be shared by the network participants. Figure 19 illustrates the centralized platooning system with Scania as the trusted central intermediary.

![Figure 19. A centralized platooning positioning system](image)

The main challenge related to a centralized system:

- Operation and maintenance of a shared centralized database
  - Who to run the intermediating entity?
  - How to share costs for the intermediating entity?

A decentralized blockchain system has the potential to solve this challenge. In such a system, there will be no central intermediary deciding the positions in a platoon. The operation of deciding and recording positions in the platoon would rather be a task for a smart contract residing on a blockchain. The smart contract would be coded in such a way that it, for a given platoon, awaits GPS signals to be sent from each platooning participant before doing some computations to establish the order of trucks. After the order has been established, the smart contract would take this information and put it in a new transaction and propagate it to the network. The process of putting this transaction in a block is a task for the platooning participants who will take turns, using a round robin consensus scheme, to put the smart contract generated transactions in a block and propagate it to the platooning community network. Only blocks containing transactions generated by the smart contract, which all participants have agreed is the correct way to compute positions in the platoon, will be accepted by the network.
Each truck in the platoon would be a node in the network holding a copy of the platooning blockchain. The blockchain would be private meaning that only invited participants could engage in the platooning network. The system would have to be able to read all transactions on the blockchain so that it can determine each participant’s contribution to the network and subsequently optimal order in the next platoon. Figure 20 illustrates a high-level view of what a decentralized platooning positioning system could look like.

Figure 20. A decentralized platooning positioning system

5.2.1 Analysis

Complexity

A decentralized system in relation to platooning positioning does not come without its implementation challenges. One fundamental aspect of the decentralized system described above is that the correctness of position data recorded in the system relies on the correctness of data generated by the smart contract which in turn depends on the correctness of GPS signals received from platooning participants. The correctness of GPS signals can be compromised due to at least two reasons where corrupt positioning data is the first and timeliness of data is the second.

Regarding corrupt positioning data, if a haulier has the competence and will to modify a truck’s software in such a way that the positioning data it transmits is off by only a little, the result could be that the smart contract calculates this truck’s order in the platoon to incorrectly be the first and by such, incorrectly record a contribution for this truck.

The timeliness of GPS signals send by platooning participants has a technical dimension in addition to the issue of participants trying to trick the system. For the smart contract to correctly compare and order GPS signals, the signals need to be sent at the exact same time. This is impossible as there is no universal clock. A slight delay in sending the GPS signal will result in the truck responsible for the delayed signal appearing further ahead than is the case. This would of course be a benefit for the truck in question as the system would think, given that the signal is delayed long enough, that it is the leading truck in
the platoon. Again, a delayed signal could be innocent in that a technological problem might cause it but it can also be caused by a participant trying to trick the system.

If concluding that the method of sending GPS positions to a smart contract is infeasible due to the problems just described, some other method needs to be used to decide the order of trucks. The solution could be to use a sort of technology that leverages the proximity of participants in the platoon. For example, each truck could have a camera installed with the task of recording the license plate of the subsequent truck in the platoon. The recording of the license plate could perhaps be made possible with Optical Character Recognition (OCR) technology. The smart contract would instead take the different licence plate numbers as input to calculate the order of trucks. Furthermore, the pictures from which the licence numbers are collected needs to be stored as proof in case of a dispute. While this approach may be feasible, it does add another layer of complexity.

Incorrect GPS signals aside, another “softer” issue might discourage the usage of a decentralized blockchain version of the system. This issue relates to the fact that positioning data would be visible for all participants in the platooning community. It is inevitable that fellow members in a specific platoon will have knowledge about each other’s positions during a platooning event but it is far from certain that hauliers would be comfortable sharing positioning data with literally all members and competitors in the platooning system.

**Value proposition**

The ability to trace positions in a platoon is believed to be essential if platooning is to gain widespread adoption. Whether a blockchain should be used depends on how important decentralization is. A platooning tracking system based on blockchain is valuable if the following two conditions are fulfilled.

- There exists no trust between network participants in regards to collectively maintaining and updating a shared distributed database with the purpose of recording the order in platoons
- A trusted intermediary, with the purpose of managing the central database, is either too costly or impossible to find.

**Corresponding centralized solution**

A blockchain can be a good solution in an environment that lacks trust. In contrast, a blockchain can be overly complicated in applications where there is trust. Both ends of the trust spectrum can be considered. If there is full trust between platooning participants meaning that the risk of a participant reporting false information is neglectable, or if a suitable trusted intermediary can be found, then a centralized approach is advisable. A centralized approach backed by trust does not even have to use any signalling by means of GPS, the system could be as trivial as letting the leader of a platoon record its contribution in a central database. If the trust in the network lies somewhere between full
trust and no trust, then a centralized solution could borrow an element used by blockchains, namely digital signatures. While data is still recorded in a database managed by a trusted authority, the system can become more credible by requiring each recorded contribution to be signed by each subsequent member in the platoon. Such a system would prevent members in the network from recording false contribution even though it still allows the possibility of members benefiting from the platoon not submitting their signatures. Finally, if there is no trust at all in the network, including any trusted third party that can maintain a central database, then a blockchain should be considered under the condition that the collective value of the system off-sets the cost of implementing it.

5.3 Provenance tracking

Provenance tracking is a term used to describe the activity of tracking the origin of an asset in a supply chain. Like many processes, provenance tracking can benefit from being digitalized. Using manual procedures to record change of ownership between different levels in the supply chain likely takes more time than if this process were to be done using digital tools. Moreover, the risk of errors is presumably higher for manual processes compared to digital processes. If a physical signature on a piece of paper is required for an asset to change ownership, then this paper must be manually processed by some other entity to effectively change the ownership. This involvement of a trusted third party may be both inefficient and costly. Also, if a mistake is made and a physical signature is missing, then the goods might be stranded between two levels in the supply chain or maybe worse, if the goods are allowed to carry on through the supply chain, despite the fact that change of ownership has not been recorded correctly, then a company further up the supply chain might pay the price for damaged goods caused by a company several levels down the chain.

As Bitcoin has been a living example of, to this date at least, a blockchain can be used to securely move the ownership of digital assets between entities in a network. Of course, one could do without a blockchain solution by using a trusted third party to record the change of ownership and this process could be made digital as well. But as already discussed in this thesis, a blockchain can provide value if we want to get rid of the trusted third party and hence, make the process in question potentially more efficient in terms of time and cost. If a blockchain were to be implemented in a peer-to-peer provenance tracking system, there are two ways to go about it.

The first approach is to leverage a sort of coloured coins protocol, as discussed in the ScaniaWallet use case, to tokenize physical assets representing the goods that are to be moved through the supply chain. If using the Bitcoin network, the manufacturer of a product that are to be moved through the supply chain can issue a digital token of that product on the Bitcoin blockchain. After the product has been digitalized and issued on the blockchain, it can be readily transferred to other network participants, or in this case; to other members of the supply chain. Miners will validate transactions in the same way
they validate normal bitcoin transactions. Their incentives to validate these transactions will be the same, i.e. to receive bitcoins.

The second approach is quite similar, except for the fact that a private blockchain would be used instead of an already existing public blockchain such as Bitcoin. If using a private blockchain, rules need to be set up regarding different aspects of the blockchain. The main aspects to consider are: who should be included in the blockchain network, which nodes should be used as validators and what kind of consensus scheme should be used to enable these validators to come to a consensus on the state of the blockchain. A public blockchain often has a lot of validators if the incentive structure is properly designed. The more validators, the more decentralized and more secure a blockchain could be considered. The validators in a private blockchain will not be as many and because of that, perhaps not as secure. However, since the real-world identities on a private blockchain is known, the security of the private blockchain can be enforced by having legal contracts signed by all network participants.

A private blockchain of this sort could for example include Scania, a manufacturer of a specific part needed by Scania, and finally the rest of the companies involved in between Scania and the manufacturer that enables the specific part to move from the manufacturer to Scania. Just like if using a coloured coins protocol, the manufacturer, i.e. the first level of the supply chain, would have permission to issue new assets, or rather digital tokens of these assets, on the blockchain.

Except for the technical details specifically inherent to public and private blockchains respectively, the rest of the implementation can be the same regardless the choice related to having an open or closed network. To identify and tokenize the physical asset that is to be moved through the supply chain, a RFID tag can be attached on the package of the part. To send the token of ownership to the next entity in the supply chain, the manufacturer simply creates a transaction detailing the asset ID that are to be transferred and the recipient’s blockchain address. This procedure of creating a transaction that moves the ownership of the asset is made for each transfer in the supply chain. Furthermore, each transaction needs to be digitally signed by both the sender and the receiver. Both parties will sign a digital contract which will serve as proof that the ownership of the asset has changed hands.

Provenance tracking is one of those use cases that immediately make sense to combine with a blockchain. The main difference between a blockchain provenance tracking system and a digital currency residing on a blockchain is that the first handles physical “off-chain“ assets while the latter handles purely digital assets which were born on the blockchain. The distinction between off-chain assets and digital assets has some implications on the degree of decentralization in the blockchain network. In the case of Bitcoin, both the issuance of bitcoins and the transactions are decentralized. While a provenance tracking system build on a blockchain can have the transfer of goods and recording of ownership decentralized, the issuance will be performed by one designated node and thus be centralized. The issuing node is responsible for the asset being correctly
issued and redeemable. The correctness may relate to attributes such as the quantity and quality of goods that the issued token represents. This centralized aspect of a provenance tracking system built on blockchain technology may or may not be a problem depending on the network and the level of trust that exists in it.

However, the main concern might not be that trust must be put in an issuer. The main concern could rather be about confidentiality, or the lack thereof. If a provenance tracking system is built on a public blockchain like Bitcoin, everyone can see every transaction made on the network. The ability to track all transactions on the network is necessary if the system is to be decentralized. For a node to know that another node has bitcoins, it needs to scan all transactions and find a previous transaction that is addressed to that node. This sort of transparency is a problem by virtue of the competitiveness that exist horizontally, and in some cases; vertically, between levels in supply chain network. Figure 21 shows an example of a supply chain network.

![Supply Chain Network Diagram](image)

*Figure 21. A supply chain network*

Competitiveness naturally exists horizontally on each level of the supply chain. With this competitiveness in mind, *Producer A* might not want to publicly display its connections to level 2, i.e. its customers, so that *Producer B* and *Producer C* can see these connections. A public blockchain would unfortunately disclose such information to the whole network. A solution to this problem might instead lie in the private blockchain approach.

A private blockchain would, unlike a public blockchain, only allow certain participants to join the network. To eliminate horizontal competition, only one participant from each level would be allowed. With horizontal competition out of the equation, another issue must be addressed in some type of supply chains. If the degree of processing between levels is low, i.e. some levels in the supply chain adds little value but has despite that been able to intermediate two levels in the network, then these operators might risk being disintermediated as a level 5 operator might suddenly realize that it can get a better price by doing business straight with a level 2 operator. If there exist vertical competition of this kind, operators knowing that their only value is to connect two levels of the supply
chain will probably be unwilling to join a blockchain network in which its limited value is likely to be exposed.

The process of forming a private blockchain network will start at some level and then work its way up. The incentives to have a provenance tracking system will grow stronger the closer to the end an operator finds itself in the supply chain as the degree of uncertainty related to where a specific part is in the supply chain is assumed to be higher the more preceding levels. The operator wishing to start a blockchain system of this sort will have to coordinate with its supplier which in turn needs to coordinate with its supplier and on it goes until all upper levels have agreed to form a private network with the intention of tracking goods.

In summary, a private blockchain seem to be the best solution if a decentralized provenance tracking system were to be implemented. As long as the first level in the supply chain issues assets correctly on the blockchain, the system should be functional from that point on. The process of moving these assets through the supply chain will be decentralized meaning that no trusted third party is needed to maintain the system.

### 5.3.1 Analysis

#### Complexity

The reason why the idea of a provenance tracking system on a blockchain is relatively easy to picture is that it is not that different from the idea of Bitcoin and other cryptocurrencies. In essence, this use case is about moving digital assets between nodes in a network. Due to provenance tracking sharing many attributes with cryptocurrencies, many vendors explicitly (e.g. Provenance [62]) and implicitly (e.g. MultiChain [63]) already offers platforms on which to issue digitalized tokens that are to be transferred in a network of nodes. Again, the technical complexity does not seem to be overwhelming. What might prove more difficult is gathering the members of the whole supply chain in one transparent network.

#### Value proposition

The ability for a company to reliably track its goods running through the supply chain is valuable for several reasons. If, for example, a delay would occur somewhere along the chain, the tracking system can readily inform the relevant parties in the supply chain and thus enabling them to take timely measures to reduce the harm caused by the delay. This is especially important if just-in-time manufacturing is used. Furthermore, from a legal standpoint, it is important to be able to determine the ownership of some goods at a particular point in time so that responsibility in the case of damage to the goods can be easily distributed.

At its core, the value in this use case lies in the ability to know, at any given point in time, where a set of goods are in the supply chain, without having to trust and pay a third trusted party to hold and share this information. A provenance tracking system can enable Scania
to track spare parts ordered for a specific truck meaning that any potential delays in delivery has the possibility of being detected early so that measures can be taken to mitigate the negative impact of the delay.

The network is likely to be formed using a bottom-up approach meaning that one organization will take the initiative by communicating its intents with its supplier. This supplier will then be asked to coordinate with its own supplier and on it goes until a satisfactory amount of supply chain levels are included in the network. If one member of the supply chain refuses to be part of the system, the chain will be broken at that point. However, the system might still be of value given that a satisfactory amount of preceding levels of the supply chain have agreed to join the network.

**Corresponding centralized solution**

A centralized system could consist of a third trusted party that runs the provenance tracking system with all supply chain participants communicating with it. For a transfer of goods between two levels in the supply chain to be considered complete, the centralized entity must receive signals from both the sender and receiver in regards to the transfer. Whatever records possessed by the centralized entity are considered to be the truth and hence, trust needs to be put in this entity in regards to the correctness of the system. If a dispute would emerge, it would be resolved by consulting the centralized entity.

Besides having to trust a third party to run the system, the network participants would also have to compensate this third party. It is unclear how the costs of buying or developing a blockchain platform compares to the cost of having a trusted intermediary running the system but given that the costs would be the same, a system relying on blockchain can offer extra value through its higher degree of decentralization.

### 5.4 Event data sharing with competitors

The ability to mutually share data among peers can prove valuable, for all parties involved, in many situations. This use case considers a decentralized blockchain system in which competitors form a network with the purpose of keeping track of how much data each participant has shared and how valuable this shared data is. The idea is that network participants will be rewarded for the data that they share if, and only if, one or several peers deem it valuable and as a result; uses the data. Due to all network nodes having to know about all transactions in the network, data will be encrypted before it is shared with only the recipient node having the ability to the decrypt it.

To understand the usefulness of such a system, one can picture a situation in which a competitor’s vehicle pick up information about poor road conditions at a specific location. This competitor realizes that this information might be valuable to other network participants and is therefore willing to share this data in exchange for a monetary reward or simply for the favour being returned sometime in the future.
In order to create a decentralized system, one can utilize blockchain technology coupled with smart contracts. The blockchain network would be private meaning that only invited and identified participants has access to the system. The minimum requirement to get the system up and running is that one entity starts the network either by buying a system from a blockchain vendor specializing in private blockchains and smart contracts, or by creating such a system from scratch. Once the system is up and running, new participants needs to be added to the system. When there is only one node in the network, the process of adding new nodes is trivial as this sole node has full control. When multiple nodes already exist in the network at the time of a new node wishing to join the network, a simple vote among participants can decide whether this node may join or not. Generally, there should be no reason to deny permission to an aspiring node given that the identity behind the node conforms to the pre-agreed rules. The network will grow stronger, more valuable and more decentralized the more nodes that are in it.

The database table that ultimately would be maintained and shared in this decentralized network would look something like the one illustrated in Table 2.

Table 2. A simplified illustration of the data held by each node in the network

<table>
<thead>
<tr>
<th>Tx id</th>
<th>Sender</th>
<th>Receiver</th>
<th>Event type</th>
<th>Size</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Scania</td>
<td>Competitor A</td>
<td>A</td>
<td>10MB</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>Competitor B</td>
<td>Competitor C</td>
<td>C</td>
<td>20MB</td>
<td>50</td>
</tr>
<tr>
<td>3</td>
<td>Competitor C</td>
<td>Competitor A</td>
<td>B</td>
<td>50MB</td>
<td>200</td>
</tr>
</tbody>
</table>

The fields in Table 2 are described in Table 3.

Table 3. Field description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx id</td>
<td>A unique transaction identifier</td>
</tr>
<tr>
<td>Sender</td>
<td>The public key of the sender. A separate table could hold mapping information between public keys and identities</td>
</tr>
<tr>
<td>Receiver</td>
<td>The public key of the receiver</td>
</tr>
<tr>
<td>Event type</td>
<td>The type of event that the shared data represent</td>
</tr>
<tr>
<td>Size</td>
<td>The size of data shared</td>
</tr>
<tr>
<td>Value</td>
<td>The value of the data shared</td>
</tr>
</tbody>
</table>
Most fields should be self-explanatory but Event type and Value requires some clarification. The idea is that all types of events do not hold the same value. For example, Event A data might be more valuable than Event B data. If that is the case, the reward for sharing Event A type of data should be relatively higher given that the size of shared data is the same. How the value of a certain event is determined is non-trivial. In the best of worlds, the value would perhaps be derived by market forces through levels of supply and demand meaning that data becomes more valuable as the latter exceeds the former. A market driven value determination model might prove difficult because of several reasons. One of the obstacles relates to data uniqueness. Since data is hidden through encryption until two parties agrees to exchange data, it will be difficult for aspiring data acquirers to differentiate between two sets of data that are being offered by two different network participants. If the sets of data are the same in terms of them recording the same event, which again; participants might have a hard time to determine, then the value associated with these sets should be the same. Still, a market value model does not seem infeasible if participants can accept that the market will not be a 100% efficient. The market model in this case can be of value even though a property such as transparency, which is typically considered one of the main pillars on which a well-functioning market rest, is lacking.

Figure 22 illustrates the part of the use case that involves smart contracts. The reason for why two contracts are needed may not be intuitive and is probably best understood by first considering a single smart contract performing the exchange of data and some reward.

Before a single smart contract is considered, some additional background to the system is given. In a blockchain network, all validating participants need to know about all transactions, or in this case; all data shared. We do not want data to be accessible by all participants because we want each sharing participant to be rewarded for the data that they share, but only if the data is downloaded by someone. The first part about accessibility is solved by encrypting the data that is shared over the network. A single smart contract could hold the encrypted data and be shared to the whole network. Only the intended recipient would be able to locally decrypt the data and as of such, the accessibility issue is resolved. However, and this is why two smart contracts are needed, the recipient could decrypt and use this data locally without telling the network that it has done so. Of course, the node could be an honest one and send confirmation that it has received the data but that cannot be assumed in a competitive environment in which trust is low or non-existent.
To solve this problem of nodes using data without telling the network and thus without rewarding the contributor, the single smart contract is separated into two. The first contract, called the “Agreement contract”, serves as a proof that the recipient has requested access to the data. No actual data is included in the first contract; it merely serves as evidence that an agreement between the two nodes has been reached. The contributing node creates this contract by first specifying the event type and the size of the data that is to be shared. Then, to prove its identity, the contributing node includes its public key together with a digital signature. Up until this point, the contract is open meaning that any node in the network can request the data by sending its public key, coupled with its digital signature, to the contract. By sending this information to the smart contract, the sending node enters a kind of binding agreement that serves as a proof that it wants to receive the data. As soon as the Agreement contract receives the recipient's public key and digital signature, it produces a new contract called the “Enforcement contract”. The Enforcement contract holds a reference to the Agreement contract. This new contract then awaits three additional pieces of information before the exchange is completed; a digital signature from the sender, the digital signature from the receiver and finally, the encrypted data.

When the Enforcement contracts is established, one of two things can happen. Either the contributor sends its signature and encrypted data first meaning that the same situation appears as in the single contract example. The receiver could simply decrypt the data locally on its hardware without sending its signature to the Enforcement contract and thus without confirming that it has received the data. The difference this time around is that the whole network holds a record (the Agreement contract) which testifies that the receiver has agreed to receive the data. While the receiver could still locally decrypt the data, and leave the network unaware, rules in the protocol would ensure that it cannot do so without suffering some kind of penalty. For example, if the receiver has not signed the Enforcement contract within a certain timeframe, the contributor gets its reward while the receiver, who has not honoured the Agreement contract, receives a penalty. The other

<table>
<thead>
<tr>
<th>Agreement contract</th>
<th>Enforcement contract</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiating parameters</strong></td>
<td><strong>Initiating parameters</strong></td>
</tr>
<tr>
<td>• Data type</td>
<td>• Agreement contract reference</td>
</tr>
<tr>
<td>• Amount of data</td>
<td></td>
</tr>
<tr>
<td>• Pub key of sender</td>
<td>• Encrypted data</td>
</tr>
<tr>
<td>• Digital sig from sender</td>
<td>• Digital sig from sender</td>
</tr>
<tr>
<td><strong>Inputs</strong></td>
<td>• Digital sig from receiver</td>
</tr>
<tr>
<td>• Pub key of receiver</td>
<td></td>
</tr>
<tr>
<td>• Digital sig from receiver</td>
<td></td>
</tr>
</tbody>
</table>

*Figure 22. A simplified version of the smart contracts*
scenario that could play out once the Enforcement contract has been created is that the receiver sends its signature first. In a similar fashion, if the contributor would fail to send its signature and the encrypted data to the contract, it would also suffer a penalty.

The process of sharing data in the system could be simplified in the following way:

1) A contributing node in the network decides that it want to share some data. It creates a smart contract called an Agreement contract that specifies the type of data (Event type), the amount of data, its public key and finally, its digital signature. The contributing node propagates this contract to the whole network with the hope that some other node wants to acquire the data.

2) A receiving node that wants the data agrees to receive the data by sending its public key and signature to the Agreement contract.

3) Once the Agreement contract has the public key and signature of a receiver, a new contract called the Enforcement contract is automatically created.

4) Within a predetermined timeframe, the contributor sends the encrypted data and its digital signature, and the receiver send its digital signature, to the Enforcement contract.

5) The Enforcement contract creates a record detailing the transaction. This transaction is then validated and included in the blockchain.

Note that all nodes in the network can be both contributors and receivers, just not at the same time.

5.4.1 Analysis

Complexity

The complexity inherent to this use case depends on the level of sophistication desired in the system. The feature of having the value of different types of data being market driven will likely be one of the major challenges if this feature were to be included. A simplified version in which all types of data hold the same value, where essentially quality of data is omitted leaving only quantity and event type as a basis of calculating total value, might be an acceptable compromise.

A non-technical challenge will be to coordinate network participants to get the system up and running. A high degree of collaboration will be needed in the case of the system being initiated and implemented by several entities. Costs related to creating the system will need to be distributed among collaborating entities as fairly as possible. Furthermore, there needs to exist a model that specifies how new participants, that may join the network at a later stage, should be charged to compensate the original innovating entities.

Value proposition

The value related to the proposed system is believed to be high for all participating entities in the network. The contributing nodes are compensated for the data they share while
receiving nodes can acquire useful data they would not be able to obtain otherwise. Nonetheless, the members of the system are competitors meaning that while compensation for data shared is positive for the sender of data, it is also negative since the receiver of data, i.e. a competitor, also benefits. The price tag a sender of data sets on its data may not be derived simply by the mechanism of supply and demand, it is also likely a function of the competitive nature between participants in the network.

For example, a large member of the network, with many vehicles in its fleet, will on average be a sender of data rather than a receiver. A large member of this kind has the luxury of collecting most of its data itself which then gives them the choice to share the data. On one hand, this member can gain an extra income by sharing the data while on the other, sharing the data would enable a competitor to offer a better service to its customers. Depending on the competitive landscape, a large entity might not want to share data at all, or it might demand unreasonably high prices for it, due to the reason that it deems the competitive edge the data provides invaluable.

Assuming that the asymmetry regarding the collection of data between smaller and larger members of the network does not pose a problem, the system will likely create a win-win situation for its users.

**Corresponding centralized solution**

Just like all other proposed use cases, the system can also be implemented by using a third trusted party that acts as a central facilitator between participants in the network. This centralized entity could provide a platform on which participants can share data. As long as all participants trust the facilitator in terms of it being independent and fair, the system has the potential to be valuable for everyone while also being fairly easy to implement from a technical standpoint as these kind of centralized solutions is a well-known type of architecture. The main downside related to using a centralized system is the cost the participants would need to absorb related to having a facilitator running the system. Another issue that might prohibit a centralized system to form in the first place could be the inability to find a suitable facilitator. Due to any of these two reasons, a decentralized solution might offer a better approach.

**5.5 Transparent communication with regulators**

One potential blockchain use case that was identified before the start of this thesis was the ability for Scania to transparently and securely share relevant data with regulators. A potential scenario where such an application could prove useful would be if regulators would like to know where Scania’s trucks are driving so that a type of road wear taxation could be enforced. As the theory section of this thesis hopefully has demonstrated, blockchains can indeed be useful as a shared database where the sharing entities does not necessarily fully trust each other. However, there are several properties that heavily reduces the value that blockchain technology could provide in this use case.
First, the fact that the data shared would origin from one source, namely Scania, is problematic. A blockchain provides no means to prevent Scania from submitting false data. While data submitted to a blockchain under the right circumstances can be considered immutable and secure, the blockchain in this use case has little value if all network participants cannot conclude for sure that the data is correct in the first place. This problem could perhaps be solved if regulators installed their own hardware in Scania’s trucks. That way, both Scania and regulators could keep track of the positioning data produced by a Scania truck. Still, it makes little sense to involve blockchain technology and the reason is the systematic superiority regulators holds over entities they seek to regulate. In case of a dispute, regulators will likely trust their own data meaning that the whole consensus mechanism inherent to a blockchain is rendered useless.

Again, blockchains should be considered when there is a lack of trust between entities in need of a shared database and where a trusted intermediary is either unwanted or hard to find. While this use case might benefit from a blockchain in the respect that regulators do not fully trust Scania, there is no benefit in using a blockchain as regulators will have the final in case of a dispute. Regulators are in a way trusted by default.

If regulators did not have their systematic superiority over Scania, then a blockchain could provide a shared database without the need of a trusted third party to maintain it, that is if one additional criterion is fulfilled. There must be at least one more node in the network to make sure that a majority has a chance to form in the case of a dispute. In this use case, that means that there must be an additional hardware piece put in place in the truck by an additional blockchain network participant. Now if one node changes the data, the other two nodes can form a 66% majority. But then one must figure out a suitable third network participant and who this should be does not seem obvious.

There is yet another issue to address and it relates to the hardware that would be installed in the trucks. For the network to be initialized to begin with, there must be some guarantee that the different hardware produces the exact same data. This will of course be extremely difficult unless a trusted party is used to manufacture and configure all hardware which of course would be contra productive to what the blockchain is trying to achieve in the first place.

5.5.1 Analysis

The analysis model used for previous use cases does not apply for this use case as it is deemed to be infeasible on a conceptual level already. But in conclusion, a blockchain appears to be a poor choice of technology if there is an imbalance in the power distribution among nodes as is the case between regulators and the entities they seek to regulate. Furthermore, if data originate from one source, a blockchain seem to offer little to no value. That is not to say that blockchains cannot provide a great tool for regulators to make their job easier in some cases. Consider a scenario where all financial activity between financial institutions is conducted on a blockchain. If regulators would be given read access to this blockchain, they can monitor all the financial activity and make sure
that no institution behaves in a way that poses a risk for the financial system as a whole. The key insight here is that the network is shared by nodes that systematically are on the same level with the regulator only having read permission to the network.

6. Discussion

There is no doubt that blockchain technology is a truly innovative technology in the sense that it enables new type of decentralized applications that simply was not possible before. The ambition at the start of this thesis work was to isolate the blockchain technology from Bitcoin, the application in which blockchain was invented. While they are distinguishable in the sense that blockchain is the underlying technology and Bitcoin is an application build on top of this technology, it is hard not to give cryptocurrencies, through Bitcoin, a vast amount of attention as it is by far the most proven blockchain application to date. The founder of Bitcoin; Satoshi Nakamoto, invented blockchain to solve a very specific type of problem, namely the one of sending value over the internet, without having to go through a trusted intermediary. Proposed use cases circulating in the blockchain space relates to this problem to various degrees. In many cases, blockchain technology seem to have been generalized one step further in such a way that it now underpins the notion of decentralized applications regardless of their objective. These use cases originate from the idea that a blockchain can, with merit, be used for everything that aims to mitigate the power of intermediaries.

While this might prove to be a valid generalization, it is still early days and it is in many cases not obvious how blockchain technology should be used to add value. A large proportion of blockchain use cases, if not all, can be implemented using a trusted intermediary and hence, the degree of novelty is limited to a potential improvement of existing procedures rather than the creation of something entirely new. The use of blockchain boils down to a technology choice with its own trade-offs relative to other possible alternatives such as a centralized database. Nonetheless, these improvements might prove to be so significant that blockchain indeed lives up to the epithet: “the next generation of internet”.

In the case of transferring digital value such as money, stocks, bond, or any other type of financial instruments, blockchain technology appears to be very promising as the technological challenges inherent to these use cases seem solvable at first glance. The fact that the transfer of financial instruments relates so much to Bitcoin is likely why it is relatively easy to imagine such use cases. However, there are also non-technological issues such as privacy and the regulatory environment in which financial institutions operates. Transactions in a blockchain system needs to be open to all the validating nodes meaning that no secrets can exist between them. While lack of privacy might be a problem in some financial applications, it might not be in the case of others. Given that the process of individuals sending money to each other does not cause privacy issues, international banks could cooperate using a blockchain so that individuals might be able to send money
across the world much faster and cheaper than today. This is essentially what Ripple [64] tries to do by having a number of partnering banks connecting to their platform. R3 [65] uses a similar approach by leading a consortium partnership with over 80 of the world's leading financial institutions and regulators with the purpose of designing and delivering distributed ledger technologies to the global financial markets.

Regardless of application or industry, collaboration is key when it comes to adopting blockchain technology which is why all proposed use cases in this thesis involves a high degree of organizations working together. ScaniaWallet requires Scania, agents and hauliers to work together while Platooning, Provenance tracking and Event data sharing requires Scania and competitors to work together. While such collaboration might be hard to orchestrate, the value inherent to decentralized application has the potential to be worth the effort. As a response, many companies emerging in the blockchain space provides a technical and organizational platform on which to collaborate. In a way, these companies are paradoxically a new type of intermediary. Nonetheless, they may still offer benefits relative to conventional systems.

7. Conclusion

In this thesis, five potential use cases supported by blockchain technology were identified. Four of them appears to be feasible while one; transparent communication with regulators, seem to be a poor use case in relation to the use of blockchain technology. All identified use cases could also be implemented using conventional, centralized databases. Whether it is advisable to use blockchain technology over a centralized architecture depends primarily on the value of disintermediation. Furthermore, blockchain technology may offer increased system robustness due to data being replicated over several nodes that are virtually located inside different trust boundaries. On the other hand, both performance and confidentiality are impacted negatively by the use of blockchain technology relative to the use of a centralized database. In conclusion, the choice between a blockchain architecture and a centralized architecture is not obvious as there seem to exist a trade-off between the two.

Table 4 shows the estimated complexity and value proposition of each use case. Technical complexity refers to the perceived difficulty related to the technical implementation of the identified use case in question. The basis of this estimation is largely a rough estimation regarding the number of platforms devoted to supplying services needed to realize the use case. Organizational complexity on the other hand refers to the perceived complexity related to coordinating the organizations that are to take part in the blockchain network. The organizational complexity is estimated to be high for all proposed use cases as they involve cross organizational collaboration, in most cases horizontally over competitive borders. Value proposition is based on the estimated value each use case would offer without comparing each use case to its corresponding centralized system. As already mentioned in this thesis, all proposed use cases could be implemented without
blockchain technology given that trusted intermediaries are used instead. No conclusions whether using intermediaries is advisable over the proposed blockchain systems is made in this thesis. If one of the proposed use cases is under consideration of being implemented, it is essential to make a thorough cost-benefit analysis relative to its corresponding centralized architecture. However, such an analysis is outside the scope of this thesis.

*Table 4. Summary of identified use cases*

<table>
<thead>
<tr>
<th>Use case</th>
<th>Technical complexity</th>
<th>Organizational complexity</th>
<th>Value proposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ScaniaWallet</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Platooning</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Provenance tracking</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Event data sharing</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Transparent communication with regulators</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

It is worth emphasizing that the degree of decentralization is not part of the value proposition estimation in Table 4 even though it is briefly discussed in the *Analysis* section of most use cases. Value proposition in this case merely refers to the value inherent to the use case regardless of its underlying technology. For example, ScaniaWallet’s value proposition estimation is based on the value inherent to Scania having its own currency, not whether the application is decentralized. This approach might seem ambiguous as both technical and organizational complexity are very much related to the decision of creating a decentralized application. The reasoning behind excluding the aspect of decentralization from value proposition is the same as why no conclusions are made regarding whether a use case should be implemented using a decentralized blockchain approach or a conventional centralized approach. A more extensive analysis in regards to the cost and benefits related to both approaches is needed to estimate the relative values between a centralized and a decentralized approach. As a result, value proposition refers to the proposed service regardless of the degree of decentralization.

Some brief conclusions regarding each identified use case are presented in the following sections.
**ScaniaWallet**

ScaniaWallet enables Scania, agents and hauliers to transact using Scania’s own currency called ScaniaCoin, thus avoiding potential fees and delays inherent to the conventional payment systems. The technical complexity is estimated to be low given that an existing blockchain platform such as Ethereum or Bitcoin can be used to implement the currency. The technical complexity related to Scania creating its own Bitcoin-type client would likely be higher but might be kept relatively low if Bitcoin’s open source code is leveraged. The highest technical complexity can be found if Scania seeks to develop their own client from scratch.

Due to uncertainties regarding ScaniaWallet’s ability to compete with existing payment systems in terms of costs, the estimated value proposition is labeled as *Medium*. On the other hand, perceived value is increased by a blockchain’s potential to process payments faster and independently of holidays and weekends, thus enabling hauliers, that are required to pay in cash, to receive service faster. However, the centralized ScaniaWallet’s potential to process payments faster is even greater as it only requires a change in a single database owned by Scania so from this perspective, blockchain does not offer an advantage.

In summary, blockchain technology’s only benefit over its corresponding centralized system is that payments are decentrally processed which means that network participants do not have to trust Scania in terms of transactions being processed correctly.

**Platooning**

A platooning system built on blockchain technology enables platooning participants to come to an agreement on the order of trucks in the platoon, without requiring a central intermediary to aid the process. The technical complexity is estimated to be high due to the technology having to be developed from scratch as there seems to be no similar service on the market. Moreover, the blockchain technology would likely have to be coupled with OCR technology to work, thus adding yet another dimension of complexity.

In terms of value proposition, a platooning ordering system of this kind is estimated to be of great value if the ambition is to maximize platooning activity. If network participants know that platooning benefits will be evenly distributed, the will to initiate and lead platoons is believed to be higher.

**Provenance tracking**

A provenance tracking system enables network participants to trace goods through a supply chain without having to rely on a central intermediary to hold and track records of ownership. The technical complexity is believed to be relatively low as different platforms already offer ways to issue tokens that can be used to represent real world assets.
The value inherent to this use case is believed to be high as higher certainty of where goods are in the supply chain increases Scania’s ability to plan orders so that potential consequences delays in deliveries might cause can be mitigated.

**Event data sharing with competitors**

*Event data sharing with competitors* refers to a system which purpose is to enable participants to share relevant data in a peer-to-peer network. Even though existing blockchain platforms can be leveraged to implement this use case, a lot of configuration is likely required and thus, the technical complexity is estimated to be high.

The ability to share and receive data in a network of competitors in a fair and safe manner is believed to benefit all actors willing to participate in the network. Participants holding large amounts of relevant data can sell data of their choice and earn a small profit. Conversely, participants that buy the data can use it to enhance the services they offer to their customers.

**Transparent communication with regulators**

*Transparent communication with regulators* is about communicating with regulating entities over a blockchain. This use case was built on the notion of a blockchain being more secure and reliant than other choices of technology, that regulators somehow could trust the data it receives from Scania to a higher extent if it was shared using a blockchain. While data distributed over several nodes using blockchain technology under the right circumstances could be considered immutable in the sense that past records cannot be altered, the correctness of data residing in the blockchain is dependent on the entity submitting the data. If entities that are to be regulated submits false data, the question should not be how to store this false data, it should be about how to prevent false data from being submitted. Unfortunately, blockchain technology does not offer an answer to that question.
References


