Information Security in an Internet of Things Network Based on Blockchains and User Participation

Anton Daniels

Computer Science and Engineering, bachelor's level
2019

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering
Abstract

The amount of connected Internet of Things devices has seen a large growth during the last couple of years and shows no signs of slowing down. Considering the momentum of the technological advancement in our society with new technologies such as blockchains, AI and machine learning, a large amount of issues could occur if not prevented beforehand, especially within security. Therefore this thesis will examine how to maintain the information security in an Internet of Things network based on blockchains and user participation, by taking an exploratory approach to create an understanding of the issues and possible solutions when implementing a network of this type.

By using a case developed together with Luleå Kommun this thesis takes a qualitative approach to the research. This is done by using solutions to issues which appeared during the development of this implementation to draw a conclusion on how to maintain the information security in an Internet of Things network based on blockchains and user participation.
Sammanfattning

Mängden anslutna Internet of Things enheter har sett en stor ökning under de senaste åren och visar inga tecken på att sakta ner. Med tanke på hastigheten av den teknologiska utvecklingen i vårt samhälle med ny teknologier som AI, maskininlärning och blockkedjor, kan en stor mängd problem uppstå om inte förhindrade på förhand, särskilt inom säkerhet. Därför kommer denna rapport undersöka hur man upprätthåller informationssäkerheten i ett Internet of Things nätverk baserat på blockkedjor och användarmedverkan, genom att använda en explorativ ansats för att skapa en förståelse av problemen och möjliga lösningar under en implementation av ett nätverk av denna typen.

Genom att använda ett användningsfält utvecklat tillsammans med Luleå Kommun kommer denna rapport ta en kvalitativ ansats på forskningen. Detta genomförs genom att använda lösningar till problemen som uppstod under utvecklingen av denna implementation för att dra en slutsats om hur man upprätthåller informationssäkerheten i ett Internet of Things nätverk baserat på blockkedjor och användarmedverkan.
Acknowledgements

I would like to express my gratitude to my supervisor Johan Wenngren who made this project possible, by proposing this idea and guiding us throughout the project. I would also like to thank the experts at Luleå Kommun who participated in the workshop.

Finally i would like to thank my partner throughout this project Robert Ljungblad who also wrote a thesis about the work made in this project
# Table of Contents

1. **Introduction**  
   1.1 Purpose/problem statement  

2. **Background**  
   2.1 Internet of Things  
      2.2.1 Front-end Proxy Solution  
      2.2.2 Gateway Solution  
      2.2.3 TCP/IP Overlay Solution  
      2.2.4 Wireless communication  
   2.3 Distributed Ledgers / Blockchains  
      2.3.1 Ethereum  
      2.3.2 Smart contracts  
      2.3.3 Consensus  
   2.4 Information security (CIA-Triad)  
      2.4.1 Confidentiality  
      2.4.2 Integrity  
      2.4.3 Availability  
   2.5 Public Key Infrastructure (PKI)  
   2.6 Similar work  

3. **Method**  
   3.1 Research Approach  
   3.2 Research Methodology  
      3.2.1 Exploration  
      3.2.2 Design  
      3.2.3 Implementation  
      3.2.4 Evaluation  
   3.3 Data Collection  

4. **Results**  
   4.1 Designing a Solution for an Internet of Things Network  
      4.1.1 Important aspects  
      4.1.2 Use case  
      4.1.3 Conceptual Solutions for an Internet of Things Network  
      4.1.4 Hardware and software used
4.2 Implementation of a Solution for an IoT Network
  4.2.1 Ruuvi-tag
  4.2.2 Mobile Application
  4.2.3 Blockchain
  4.2.4 Decentralized Application

4.3 Limitations

5. Discussion
  5.1 Confidentiality:
  5.2 Integrity:
  5.3 Availability:
  5.4 Bonus system
  5.5 Important aspects
    5.5.1 Availability
    5.5.2 Communication
    5.5.3 Cost
    5.5.4 Incentive
    5.5.5 Maintenance
    5.5.6 Security
    5.5.7 Usability

6. Conclusion

References
  Books and papers
  Websites
1. Introduction

The Internet of Things is supposed to revolutionize the way we interact with technology and will fundamentally change the way we live our lives (O'Sullivan, 2018). Internet of Things has seen a big growth during the last few years and is set to skyrocket in the next couple of years.

There are a large number of issues that can occur in IoT networks, for example around wireless communication. With the amount of wireless communication in our society is increasing, the amount of network traffic is also increasing, which could lead to wireless signals interfering with each other. Cost is also a problem, where there could be hard to create an entire IoT network that is both cost and resource efficient. To solve these problems, the main focus of research and development are around there areas (OECD, 2015):

- Security, to keep the system secure
- Integrity, to keep the users personal information secure
- Reliability, to keep the functionality of the system secure for a long period of time
- Range, to make sure the connection reaches far enough for its geographical position
- Cost, to make sure the solution is affordable
- Energy efficiency, long battery time etc.

Table 1 below describes the results of an investigation made by the research and advisory company Gartner in the beginning of 2017. According to this investigation there would be 8.4 billion connected devices worldwide in 2017, which would be an increase by 31% compared to 2016. Gartner also estimates the amount of connected devices would reach 20 billion in 2020.

<table>
<thead>
<tr>
<th>Category</th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer</td>
<td>6 930,0</td>
<td>5 244,3</td>
<td>7 036,3</td>
<td>12 863,0</td>
</tr>
<tr>
<td>Business: Cross-Industry</td>
<td>1 102,1</td>
<td>1 501,0</td>
<td>2 132,6</td>
<td>4 381,4</td>
</tr>
<tr>
<td>Business: Vertical-Specific</td>
<td>1 316,6</td>
<td>1 635,4</td>
<td>2 027,7</td>
<td>3 171,0</td>
</tr>
<tr>
<td>Grand Total</td>
<td>6 381,8</td>
<td>8 380,6</td>
<td>11 196,6</td>
<td>20 415,4</td>
</tr>
</tbody>
</table>

Table 1: IoT Units Installed Base by Category (Millions of Units)(Gartner, 2017)
This is a large growth in a short period of time, which is a sign of our technology advancing. Such a large growth could as mentioned earlier cause issues, therefore aspects of the Internet of Things concept needs to be examined before it’s too late. One significant aspect that needs to be addressed are the security issues that comes with an Internet of Things solution (Burgess, 2018), if those issues are not solved in the near future we could end up with severe problems. For example some devices can have flawed security solutions which can result in intruders taking control over parts or even the whole network. This is especially dangerous considering the growth of the number of connected devices and the pace of our technological evolution. Especially with new concepts emerging like AI and machine learning, which can result in a technological advancement our society isn't ready for.

One emerging technology that has gained popularity in the last couple of years, which could contribute solutions to some of these problems, is the distributed ledger technology. Or more specifically the blockchain technology which is based on the distributed ledger technology. The distributed ledger technology is a database that exists across several locations or among multiple participants (Tradeix, 2018), compared to the currently most common solution which is using a single centralised database. A blockchain distributed ledger that consists of “blocks” containing information that get added to a chain of transaction records, which uses a cryptographic signature called a hash to connect the blocks together.

A big component of the blockchain technology is that blockchains is that anyone can view the contents of the blockchain and can choose to connect their computer to the blockchain network (Investopedia, 2019). When a computer is connected to the blockchain network the computer gets a copy of the blockchain that is updated when a new block is added to the blockchain. Since every user has an identical copy of the blockchain it makes is difficult to manipulate the data that is already stored on the blockchain. Another thing that makes attacks to a blockchain difficult is the chain part of the blockchain. The hash is used to connect the blocks together by referring to the previous block and an attacker manages to change the information on a block, that block will then generate a new hash. This means the block is no longer a part of the chain since all the blocks after this block is referring to the unchanged hash value. Therefore the attacker will need to change all of the blocks that comes after the changed block, which can be incredibly difficult to do.

Considering the earlier mentioned issues that could occur in IoT networks, the blockchain technology could be a solution to some of the problems within security. That is why in this thesis the blockchain technology will be examined in regards to an Internet of Things network.
1.1 Purpose/problem statement

The purpose of this project is to create an understanding on how blockchain technology can support the communication and security in an Internet of Things network.

This is done by creating a conceptual Internet of Things solution that makes it possible to transfer information from sensors even if the sensor does not have internet access through for example the mobile network of WiFi. In this project a case was developed together with Luleå kommun. Luleå kommun owns and manages around 650 public waste bins. This project was developed to help Luleå kommun improve both their resource and time efficiency when planning and executing their bin emptying routes. The idea of the project is to place a wireless sensor in a trash can which will communicate with nearby mobile devices when it’s time to empty the bin. This information would be handled by a mobile application that sends the information to a blockchain, which later can be accessed by the municipality to reduce the amount of resources spent while emptying the waste bins.

To examine how blockchains can contribute to create a network for IoT built by user involvement the following problem statement will be used:

- How do you maintain the information security in an internet of things network based on user participation?
2. Background

This section will give the reader some context about the technologies and terminologies used in this thesis. This context is provided to help the reader get a better understanding of how the results were reached and what is discussed in the end of the thesis.

2.1 Internet of Things

The term Internet of Things (IoT) is most commonly used to describe objects that communicates with each other. For example a thermostat that can be controlled by using an application on your phone (Burgess, 2018), or most of the things that can be controlled with a phone such as lights, hot tubs, cars and so on. These object doesn't necessarily have to be controlled by a phone. Some objects are more automatic, for example a coffee maker that starts in the morning when your alarm starts. A real world example of this is the new “Home Connect” system developed by Siemens where the user can control its appliances through a mobile application, which can for example give the user a notification when the laundry is done or the user can view the inside of the fridge with help of cameras inside the fridge (Siemens , 2019).

The devices in an IoT system are most typically run by a tiny chip in the device. The device itself is not that smart, but it is linked to a proper computer or a system of computers which allows it to access information from other sources which makes the chip “smart” (O’Sullivan, 2018).

If we use a coffee maker as an example it already has all the usual parts coffee makers are equipped with. The coffee maker will also be equipped with some small computer hardware, such as a small motherboard, processor, network card and some sensors. This makes it able for the coffee maker to connect to the internet and access information that makes it possible for the coffeemaker to communicate with other devices. This is usually controlled på by a control device, which most commonly is a mobile phone. Ideally you want to be able to control everything using the same application on your phone but since there are a lot of different companies developing these devices there are usually different application for each device.

Connecting a device to the internet can be done in many different ways and can be categorised in three categories Front-end Proxy Solution, Gateway Solution and TCP/IP Overlay Solution (Yang, 2014).
2.2.1 Front-end Proxy Solution

In this solution the connection is performed by a middleware proxy and there is no direct connection between the device and the internet. This is done by having the proxy collect and store the data while the user access the data from the proxy by using queries such as SQL queries or web based interface.

2.2.2 Gateway Solution

This solution uses a gateway that is located between the device and the internet. The gateway performs tasks such as protocol conversion and message relay to help the device and the internet hosts to directly communicate with each other.

2.2.3 TCP/IP Overlay Solution

This solution uses an overlay network constructed on either the device or the internet. This is done by implementing a TCP/IP protocol stack above a microcomputer system in the device to assign an IP address to the device.

2.2.4 Wireless communication

An important part of IoT networks is the wireless communication. Therefore four different types of communication that could fit as a solution when creating an Internet of Things network of this kind was explored, these four were:

- Radio Frequency Identification (RFID), a one-way communication protocol which uses small tags that broadcast their location. (OECD, 2015)
- Near-Field Communication (NFC), a two-way communication technology which is commonly used for interactions such as payments or entering a facility. (OECD, 2015)
- Bluetooth, which initially was designed as a wireless personal area network to connected devices such as mouses and keyboards at short range to mobile phones and computers. Bluetooth has in later years expanded to support low-energy profiles by using low energy sensors and tags. (OECD, 2015)
- LoRa, a long range, low power wireless platform. LoRa is used to generate a Low power wide area network (LPWAN) making it possible for IoT devices to connect to the internet in regional, national or global networks (Semtech)
2.3 Distributed Ledgers / Blockchains

When storing information on a network centralized ledger systems are most commonly used, where the system is controlled by a central mechanism, such as a database, and then transmits the information other users on the network. This means all users on the network are dependent on the central mechanism to take any actions (State of the DApps, n.d.). Since this creates a single point of failure on the network and the increasing interest from users to keep their data safe, other ways to store and control the information on a network have increased in popularity. These systems are called decentralized systems and distributed systems. Decentralized systems are controlled by multiple users connected to each other using peer-to-peer and distributed systems are also decentralised where every user executes and records the same transactions (Ethereum Community, 2016).

This technology could also eliminate the need for a third party in situations where third parties are typically needed, such as a financial transaction. The distributed ledger technology is therefore used by enterprises to validate or authenticate transactions or other types of data exchanges. These records are stored in the ledger when they have been approved by the parties involved. All the information stored in the distributed ledger are given timestamp and a unique cryptographic signature and can be viewed by all of the participants in the ledger. This technology provides a verifiable and auditable history of all the information stored on that particular dataset (Tradeix, 2018)

The most commonly known example of the distributed ledger technology is Bitcoin. Bitcoin is a cryptocurrency that is built by using the blockchain technology, which is a type of distributed ledger. Bitcoin was first described in the paper “Bitcoin: A Peer-to-Peer Electronic Cash System” written by bitcoins creator in 2008 (Nakamoto, 2008). Even though the use of blockchain in more generic ways was described in Nakamoto's paper, it was not until a few years later that blockchain technology started being used as a generic term (Ethereum Community, 2016). A blockchain is a distributed computing architecture which as mentioned earlier is a system where every node on the network executes and records the same transactions, these transactions are grouped into blocks. Only one block can be added at the time and contains mathematical proof that verifies that it follows in sequence from the previous block.
These “blocks” are made of three different kinds of digital pieces of information. (Investopedia, 2019)

1. Information about the transactions, such as sensor data, date and time etc.
2. Information about who is participating in the transaction, such as a unique cryptographic digital signature which is used instead of personal information such as your real name.
3. A unique cryptographic signature called “hash” which distinguishes the block from other blocks. For example if the users sends two identical transactions these two transactions will still have different hashes and will be distinguishable from each other.

When bitcoin started to attract attention from developers and technologists, people started to explore the use for the bitcoin network for other purposes. In 2014 a group of developers began working on a next-generation blockchain with the capability to be reprogrammed to perform any arbitrary complex computation. This blockchain created is called Ethereum (Ethereum Community, 2016).

2.3.1 Ethereum

Ethereum is a programmable blockchain that allows users to create their own operations of any complexity, rather than using pre-defined operations such as bitcoin transactions (Ethereum Community, 2016). Ethereum refers to a suite of protocols that define a platform for decentralised applications. At the heart of this is a runtime environment for smart contracts called the Ethereum Virtual Machine (EVM). The code running inside the EVM is isolated, which means it has no access to network, filesystem or other processes. The smart contracts even have limited access to other smart contracts (Ethereum Community, 2016).

The basic unit of the Ethereum blockchain is the accounts, whereas the Bitcoin blockchain was purely a list of transactions (Ethereum Community, 2016). The Ethereum blockchain tracks the state of every account and all state transitions on the blockchain are transfers of value and information between the accounts. There are two types of accounts on the Ethereum blockchain.

First there is the externally owned Accounts (EOAs), these are controlled by human users that can control the private keys which give control over an EOA. The second type of accounts is the contract accounts, these are controlled by the internal code. If the contract accounts are controlled by and human users it is because they are programmed by being controlled by an EOA with a certain address.
2.3.2 Smart contracts

The code in a contract account is referred as the term “smart contract”. Smart contracts are scripts which are triggered by addressing a transaction to it (Christidis & Devetsikiotis, 2016). When triggered the smart contract is executed independently and automatically on every node in the network through the VM, which is the EVM in the ethereum blockchain. Smart contracts makes it possible for general purpose computations to occur on the blockchain. Smart contracts especially excel when managing data-driven interaction between members of the network.

A smart contract can be defined with functions that handles data given and stored on the blockchain. For example a contracts is deployed on the network with three functions. Two of these functions can only be accessed by using the admins private key. These functions are a “Deposit” function where the admin can deposit units of asset X to the contract and a “Withdraw” function where the admin can withdraw all the assets that the contract holds. The last function is used by the other members of the network “Trade” where the users can trade 5 units of asset Y with 1 unit of asset X from the contract.

In this scenario there are three different transactions that occurs. Firstly the admin uses the “Deposit” function to deposit 3 units of asset X to the contract. Secondly a user on the network uses the “Trade” function to trade in 10 units of asset Y for 2 units of asset X. Lastly the admin uses the “Withdraw” function to withdraw all of the assets held by the contract, which is 1 unit of asset X and 10 units of asset Y.

The smart contract is stored as bytecode on the blockchain network. To decode the bytecode an application binary interface (ABI) is required. The ABI is a data encoding scheme used in Ethereum which defines how the contract information is structured. If a user wants to use a smart contract's functions it will need to have access to the ABI.

2.3.3 Consensus

In a distributed system it is important to create trust between the users, therefore reaching a consensus between the users is an important challenge. There is no central node that ensures ledgers on the distributed nodes are all the same (Zheng, Xie, Dai, Chan & Wang, 2017). Because of this protocols are needed to make certain that ledgers in the different nodes are consistent.
There are different approaches to reach a consensus in a blockchain, one approach which are used in the Bitcoin and the Ethereum network is proof of work. In proof of work each node calculates a hash value of the block header. This value must be equal or lower than a certain value. When one node calculates an acceptable value, it broadcasts the block to the other nodes and all other nodes must validate the hash value of this new block. The block is then appended to the other users blockchains. Nodes that calculate these hash values are called miners and the proof of work procedure is called mining.

Valid blocks could be generated simultaneously, this creates different branches of the blockchain. However there it is a low chance the branches will generate their next blocks simultaneously as well, Therefore the branch which becomes longer will become the authentic chain and all miners will start using that branch.

Some other approaches to reach consensus on a blockchain network are Proof of stake, which is an energy saving alternative to proof of work where miners can stake an amount of currency to participate as a validator. Proof of Authority which is a modified version of proof of stake where selected nodes creates and validates blocks.

2.4 Information security (CIA-Triad)

Since an IoT-network makes use of a lot of data from the users and devices while the devices are communicating with each other. It is important to keep this data secure, That is where the term information security is used. In a general sense, information security means protecting the assets from attackers invading the networks, such as viruses/worms, natural disasters, adverse environmental conditions, power failures, theft or vandalism (Andress, 2014).

There is a famous quote by Eugene Spafford, an American professor of computer science and computer security expert that states: “The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts” (Dewdney, 1985). This quote describes the problems that occurs while trying to secure the information in a network. The scenario described in the quote will have a very high level of security, but at the same time this scenario is incredibly impractical and the level of productivity would be near zero. That is because as we increase the level of security, the level of productivity will usually decrease (Andress, 2014). The goal therefore is finding the perfect balance between protection, usability and cost.
A big challenge when working with information security is defining when the system can be considered secure. Even if the users have updated systems, strong passwords or even if the user is completely disconnected from the internet, the users could still not be considered as secure (Andress, 2014). If the system is updated there will always be new attacks the system is vulnerable to. If the password is strong, there will be other routes for attackers to exploit. Even if the user is disconnected the system could be physically attacked. Even if it's hard to define when the system is secure it is much easier to define when the system is considered insecure, a few examples of ways to not have a secure network are:

- Not updating the system to protect from new threats
- Using weak passwords (e.g. “password” or “12345”)
- Using wireless networks without encryption

This list could get extremely long but this is not a bad thing. If the weaknesses of a system can be pointed out, these weaknesses can be handled to create a more secure network. Even if there may never be a way to achieve a truly secure network, handling these weaknesses is definitely steps in the right direction (Andress, 2014).

The primary concepts of Information security is categorised in three different categories: confidentiality, integrity and availability. This is also known as the CIA-triad and these three categories will be described now.

### 2.4.1 Confidentiality

The confidentiality concept is similar to privacy and states that the information should be kept secret or private. Confidentiality states that only authorised users should be able to access information, assets, etc that shouldn't be accessed by everyone. Identification and authentication are commonly used to make sure an authorised user is accessing the information (Rouse, 2014).

This is typically done by having some sort of authentication method to identify the user in a more secure way than just the user using its username and password. Some authentication methods used are biometric verification, security tokens, key fobs, soft tokens and the most commonly used two-factor authentication. But even the network has a good identification and authentication system there is still a risk that the information could be stolen on the way to the user, that's why it is usually a good idea to encrypt the data that is sent in the network.

There are multiple ways where the confidentiality of a system could be compromised. For example if a person is looking over a user's shoulder while typing his password, email attachments being sent to the wrong person, pieces of hardware containing information getting lost/stolen or an attacker manages to penetrate the system (Andress, 2014).
2.4.2 Integrity

Integrity states that the information should not be tampered when it is traveling or is stored in the network to maintain the trustworthiness of the data. This is typically done by having access controls, file permissions and by using accepted methods to change the data that is stored or in transit (Rouse, 2014). Most system also have backups in case of erroneous changes in the system, by either users or non-human-caused events such as an electromagnetic pulse or a server crash. A common way to secure data while in transit is “one way hashes” where a hash of the data or a part of the data is calculated before the data is sent (Infosec institute, 2018). The hash is then sent together with the data and the recipient hashes the same part of the data it has received and compares it with the original hash. If the hashes aren’t identical the message has been altered while in transit.

2.4.3 Availability

Availability states that the services should always be available, such as the systems used to store and process the information, the security aspects of the network and the communication channels used in the network (Rouse, 2014). The availability of these services are typically at risk when attacked by an attacker which are commonly referred to as a denial of service attack (DoS) (Andress, 2014). This could also be caused by non man made events such as natural disasters. The integrity of a system in typically secured by having multiple server sites that may already be running or just exists as a backup.

2.5 Public Key Infrastructure (PKI)

PKI is a set of hardware, software, policies, processes and procedures required to create, manage, revoke, distribute, use and store digital certificates and public keys (Thales Security, n.d.). PKI enables use of technologies such as digital signatures and encryption in a network with a large amount of users. PKI is often used to secure business environments which requires trust such as e-commerce and is commonly used for IoT networks.
2.6 Similar work

To gain knowledge and inspiration two different scientific papers on integrating IoT devices with the blockchain which were useful to the work in this thesis were explored, these two papers are summarised below.

In the paper “Work-in-Progress: Integrating Low-Power IoT devices to a Blockchain-Based infrastructure” (Özyılmaz & Yurdakul 2017) the authors Kazım Rıfat Özyılmaz and Arda Yurdakul described a proof of concept to enable low.power, resource-constrained IoT devices accessing a blockchain based infrastructure. This was done by using a LoRa device configured as a blockchain node to act as a gateway in a private ethereum network.

In the paper “Using Ethereum Blockchain in Internet of Things: A Solution for Electric Vehicle Battery Refueling” (Sun et al., 2018) the authors explored a solution to problems caused by limited resources of IoT devices by using an Ethereum based rich-thin-clients IoT solution. This solution made use of “Rich clients” which are full blockchain nodes and “Thin clients” which are lightweight blockchain nodes. The idea of thin clients makes it possible for lightweight IoT devices to connected to the blockchain network without doing any heavy work.
3. Method

This section contains a description on how the project was carried out. This is done by first describing the research approach taken to create an understanding of the issues and possible solutions when creating an IoT-network based on blockchains and user participation. The method used to create this understanding is later described in the research methodology chapter. Lastly this section is concluded with a description of the different methods used to collect data.

The project was performed together with Robert Ljungblad, where this thesis will focus on the broader look over the information security in the IoT-network developed in this project. To get a better understanding of the blockchain implemented in this solution, feel free to read the thesis “Blockchain in a Internet-of-Things Network Based on User Participation” (Ljungblad, 2019) written by Robert Ljungblad.

3.1 Research Approach

Since the combination of Internet of Things, blockchains and user participation is a relatively new idea, the amount of knowledge in this particular area is limited. Therefore it is unclear where the issues lie and where to look for possible solutions. Hence this thesis takes an exploratory approach to create an understanding of the issues and possible solutions when implementing blockchains and user participation into an Internet of Things network.

By using the Luleå Kommun case this thesis also takes a qualitative approach to the research. This is done by using solutions to issues which appeared during the development of this implementation to create a better understanding of these technologies.

The active participation in the development of both problem formulation and problem understanding with corresponding is a process that can be seen as action design research.
3.2 Research Methodology

As described in figure 1 below, this project follows a design process inspired by action design research (Sein, Henfridsson, Purao, Rossi & Lindgren, 2011) which consist of 4 phases: These phases are Exploration, Design, Implementation and Evaluation, and will be explained more in detail later in this section.

![Figure 1: Visualization of the 4 phases used in the design process](image)

3.2.1 Exploration

The goal of the exploration phase is to increase the knowledge surrounding the problem and finding possible solution by gathering information. This was done by first having a workshop with Luleå Kommun which were interested in the problem, to create a better understanding of where issues could appear. After the workshop a literature study was performed by reading studies about surrounding subjects, technologies, scientific papers covering problems similar to the focus of this given problem and exploring different options of hardware and software which could be used in an implementation of an internet of things network based on blockchains and user participation.

3.2.2 Design

The goal of the design phase was to design possible solutions to an internet of things network based on blockchains and user participation by using the Luleå Kommun case. This was done by using the knowledge gained in the previous phase and generating a list of important aspects. The different solutions created was later discussed to achieve the best possible solution. This phase also included choices of hardware and software used in the implemented solution.
3.2.3 Implementation
During the implementation phase the design for the solution was implemented. This was done by following the design while programming and setting up the hardware and software used in the solution. During this phase it was allowed to go back to the design phase when problems or better ideas where discovered.

3.2.4 Evaluation
The goal of the Evaluation phase was to analyse the solution created during this project. This is done by testing, discussing and comparing the solution compared with the main problem statement in this thesis with the help of the knowledge gained in the first phase.

3.3 Data Collection
Data was collected by different methods throughout all the different phases of the project. These different methods are described below.

The first method used to collect data was by a workshop held together with Luleå Kommun. This workshop was carried out together with experts from Luleå Kommun which explained their problem and help form a case by describing what the would want in a possible solution. Throughout the project continuous informal meetings were had with Luleå Kommun to get ideas for the development of the solution.

Furthermore, A literature study was performed by researching similar problems and solutions to give a better understanding of the problem and a good foundation for the solution. This started with a broad search on Google Scholar for different keywords such as “Internet of Things”, “Blockchains” and “Information security”. As the study progressed the became more refined to find more specific results.

Lastly, the hands-on experience during the implementation and debugging made in the implementation phase of the project is also a valuable data source. The issues occurred during the implementation as well as the solutions to these issues are part of the exploratory research process.
4. Results

The results section will consist of the results of the different data collection methods as well as a description of the final implemented solution. This is done by first describing the results from when designing a solution given the data collected from the workshop with Luleå Kommun as well as the literature study made in the exploration phase of the project. The second half of this section describes the result of the implementation phase as well as the data collected during this phase.

4.1 Designing a Solution for an Internet of Things Network

While designing a solution for an IoT network several different actions were taken. Firstly to help define where the focus searching and solving should lie, a list of important aspects was created as well as the creation of a use case for the system. When the important aspects were established the development of different designs of a conceptual solution was started. This was done by developing two different solutions which were compared to find the optimal solution for the use-case. The choices of hardware and software used as well as the limitations of the project is described in the end of this section.

4.1.1 Important aspects

To help define where the focus for problem searching and solving should lie, a list of important aspects was created. This list was created by using data collected from the workshop with Luleå Kommun as well as the literature study. The list was used to help with designing a solution for a decentralized network based on user participation. This list is currently incomplete, although the list is a start to help create an understanding of the problem.
• **Availability**
  ○ Data and services should always be available. Network communication and application availability should have as high uptime as possible.
  ○ The network should not rely on a third party to be maintained. The removal of the need of a third party makes the network neutral and available to several different actors.

• **Communication**
  ○ The network has to be delay-tolerant because it cannot support real time updates due to the fact that it relies on humans to pass by the sensors and collect the data.

• **Cost**
  ○ It should be free to participate in the network.
  ○ Sensors should be cheap. Preferably less than 20 euro per unit.

• **Incentive**
  ○ Any kind of participation should be rewarded to create a win-win situation for all users
  ○ Data collectors are rewarded with bonus points which can be redeemed for items or services, for example discounts.
  ○ Sensor owners are rewarded with collected sensor data.
  ○ Sensor owners get access to a relatively cheap communication network.

• **Maintenance**
  ○ Sensor battery life should be long. Preferably longer than 1 year.

• **Security**
  ○ Data should be tamper-proof.
  ○ Users should be able to trust that other users are who they say they are.
  ○ Wireless communication should be encrypted.
  ○ User integrity should not be compromised.

• **Usability**
  ○ Both applications and smart contracts should be open source.
  ○ For data collectors: application that displays their information such as account address and bonus points.
  ○ For sensor owners: application that displays collected sensor data.
  ○ Mobile application energy consumption should be low to not affect mobile phone battery life.
  ○ Mobile application memory storage requirement should be low to not fill mobile phone memory.
  ○ New users should always be allowed to join the network.
4.1.2 Use case

By using the knowledge gained through the workshop with Luleå Kommun and the literature study as well as the previously described list of important aspects, a use case could be developed. Which is described visually in figure 2 below. A waste bin is equipped with a wireless sensor which broadcasts to nearby mobile devices how full it is. When a user of the system passes by the waste bin their mobile phone will receive the information given by the waste bin. An application on the mobile phone packages the information and uploads it to the blockchain when the mobile phone has an acceptable internet connection. When the information has been uploaded the user of the mobile application will receive bonus points from the blockchain, which can be spent on, for example discounts. The users of the application can view their bonus points balance as well as their account information on the mobile application, while the sensor owners, Luleå Kommun, can view the collected data on their computers through a decentralized application, such as a website.

![Figure 2: Visualization of the use case](image)

4.1.3 Conceptual Solutions for an Internet of Things Network

During the design phase of the project two different possible solutions was designed. The general idea of these solutions having a sensor with a unique ID which broadcasts information via wireless communication to nearby mobile phones. These phones packages the information given, creates a transaction and sends it to the blockchain. This information then stored on the blockchain and can be viewed by a user through a webpage. These two different solutions is described in detail below as well as which of the 2 solutions were chosen to be implemented and why.
The first solution follows the following structure, where a sensor transmits information to a mobile application. The mobile application packages the information and sends it to the blockchain. This information can later be viewed on a web interface.

![Diagram of data flow](image)

**Figure 3: First Conceptual solution**

The sensor broadcasts data to the nearby mobile phones via wireless communication. This data includes:
- A method for identification, such as an ID-number of MAC-address
- A Data-Value, The data collected by the sensor
- A timestamp of the time when the data is sent

The main function of the mobile application is to receive data from the sensor and use the data to send a "transaction" to the blockchain.

The mobile phone should have a “light” version of the blockchain which makes it able to be a part of the blockchain network without having to store big parts of the blockchain in memory or participate in any mining. This way the blockchain itself does not require to be stored in the storage of the mobile phone, which saves a lot of hard drive space and reduces the amount of power usage and use of computing resources such as the cpu or gpu.

Excluding the main function of the mobile application there is also other functions needed on the application. The mobile application will therefore consist of three different pages, a frontpage, a user page and a settings page.
The frontpage will consist of two buttons, “SEND TRANSACTION” and “SEND DATA”, as well as a log describing the users transaction history and upcoming transactions. Since this is a test solution the application will consist of these two buttons instead of automatic transactions to simplify the testing process. On the profile page the user can see its profile with the reward level of the user and the rewards earned by the user. Finally the settings page will consist of different settings for example turn on/off notifications, change user and clearing the users history to save space on the mobile phone.

The blockchain receives transactions from the mobile application and stores the data on the blockchain depending on the information the transaction contains. The data saved on the blockchain is SensorID, Time Sent, Data-value, information about the sender (i.e which mobile phone or user sent the transaction) and when the transaction was sent to the blockchain.

Website that fetches information from the blockchain such as sensor ID, timestamp and temperature, and displays it on a webpage.

The second solution is similar to the first solution, where the difference is a gateway between the mobile application and the blockchain. The gateway is used to create a connection between the mobile application and the blockchain in case there is no possible way to implement any kind of blockchain on the mobile application, or if the blockchain results in an excessive amount of work for the mobile phone. The gateway is a server which is connected to the blockchain network, communicates with the mobile phone and handles the transactions itself instead of the phone.
The design chosen to be implemented was the first solution. This is done because of two major reasons. First of all a solution to implement a “light” version of the blockchain on the mobile phone was found. The first solution was also more of a decentralized solution compared to the gateway-solution. This is because of the gateway bottlenecking the communication which makes it a more centralized solution.

4.1.4 Hardware and software used

While designing the solution choices of what hardware and software to use was made. To help give an understanding of why these different hardwares and softwares was chosen, the reasoning behind these choices will be described.

During the exploration of the four different wireless communication options mentioned earlier in this thesis, a few problems were found making some of the options not suitable for this given scenario. Such as RFID and NFC having a very short range, and LoRa being more suitable solution for a larger scale solution with use of gateways and without user participation such as the scenario given in the report “Work-in-Progress: Integrating Low-Power IoT devices to a Blockchain-Based infrastructure” (Özyılmaz & Yurdakul 2017). Therefore the communication in this solution will consist of bluetooth. Bluetooth is suitable in this current case because there is a large amount of bluetooth devices which can be run with low energy consumption while also being relatively cheap.

The sensor used in this solution is a Ruuvi-tag. The Ruuvi-tag is Bluetooth Low Energy sensor created by a the finnish startup Ruuvi. The Ruuvi-tag is originally designed as a sensor to measure weather conditions and has a built in system to broadcast information such as temperature, humidity, pressure and motion information to a mobile phone via Bluetooth Low Energy. This sensor was chosen mainly because it is open source which makes it easier to tailor the sensor to our solution as well as its price where a Ruuvi-tag cost around 30-20 euro, depending on the amount of units bought. Since the Ruuvi-tag runs Bluetooth Low Energy and does not have an internet connection which makes this a good fit for this case solution as well as efficient, having a battery life of up to several years.
The blockchain is created by using the Ethereum network and the web interface is done as a “Decentralized Application”. These two parts of the solution are described in more detail in the report “Blockchain in an Internet-of-Things Network Based on User Participation” (Ljungblad, 2019)

The mobile application designed in this solution is an android application and is developed in android studio with the use of Go Ethereum to communicate with the blockchain

4.2 Implementation of a Solution for an IoT Network

The implementation phase resulted in a final test solution of the problem. This solution follows the structure shown in figure 7 below, which is the same structure as designed earlier in the design section. The solution consists of a Ruuvi-tag as the sensor, an Android mobile application, an Ethereum blockchain and finally a Decentralized Application that serves as a web interface. These parts will be shown more in detail in this section.

![Figure 7: Final implemented design structure](image)
4.2.1 Ruuvi-tag

The Ruuvi-Tag measures weather conditions and transmits the data to nearby mobile devices via bluetooth low energy. The data accessible from this device is temperature, humidity, pressure, motion information and the Ruuvi-tags MAC-address.

4.2.2 Mobile Application

The mobile application is an android application made in Android Studio and uses the Go-Ethereum library to communicate with the blockchain.

As seen in figures 8.1, 8.2 and 8.3 below the mobile application was developed with the planned design in mind, with a few interface and functionality changes that were made during the implementation phase.

![Visualization of the frontpage of the mobile application](image)

**Figure 8.1, 8.2, 8.3:** Visualization of the frontpage of the mobile application

Figures 8.1, 8.2 and 8.3 shows the finished frontpage on the application. As we can see the functionality on this page is similar to the design, the few changes made was that the users history was moved to the profile page and a box with IP and port has been added to help with the connection to the blockchain.
Figures 8.1, 8.2 and 8.3 show the process of data collection which occurs when a user presses the collect data button. When the data collection process starts the text of the button changes from “COLLECT DATA” to “SCANNING...” while this is happening results of the scan start showing. These results show the MAC-address of the Ruuvi-tag which sent the data received, the temperature value sent by the Ruuvi-tag and the timestamp of when the mobile application received the data. After 15 seconds the data collection process finishes the text of the button changes back to “COLLECT DATA”.

To send the data received to the blockchain the user presses the “SEND DATA” button. When the user presses the button the code described in figure 9 below will be executed.

```go
for RuuviTag ruuvi : ruuviTags) {
    transactOpts.setNonce(nonce);
    Interfaces params = Geth.newInterfaces(3);
    Interface ruuviAddress = Geth.newInterface();
    Interface ruuviTemp = Geth.newInterface();
    Interface ruuviDate = Geth.newInterface();

    ruuviAddress.setString(ruuvi.getAddress());
    ruuviTemp.setInt32((int)(ruuvi.getTemp() * 100));
    ruuviDate.setString(ruuvi.getDate());
    params.set(0,ruuviAddress);
    params.set(1,ruuviTemp);
    params.set(2,ruuviDate);
    contract.transact(transactOpts, "updateThing",params);
    nonce = nonce +1;
}
```

**Figure 9:** Go Ethereum code used by mobile application to transmit data to the Ethereum blockchain

This code is written with the use of the Go Ethereum library and creates a transaction for each Ruuvi-tag found when scanning with 3 inputs, The MAC-address of the ruuvitag, the temperature given by the Ruuvi-tag and the timestamp of when the mobile received the data from the Ruuvi-tag. This transaction is then sent to the blockchain where the data will be saved if the “updateThing” function in the smart contract accepts the given data.
**Figure 10.1, 10.2:** Visualization of the mobile applications profile page before and after establishing connection with the Ethereum blockchain

Figures 10.1 and 10.2 above show the profile page of the mobile application before and after establishing a connection to the blockchain. On the profile page the user can view its history of past transactions to the blockchain, which is stored locally on the mobile application making it accessible when offline. The Reward points used for the bonus system on the other hand is stored on the blockchain and is therefore not accessible while offline. This is accessed by using a call method to access data given by the “getBalance” function in the smart contract.

4.2.3 Blockchain

The blockchain in this solution is a private blockchain in the Ethereum blockchain network and is developed Robert Ljungblad and is described in more detail in his thesis “Blockchain in a Internet-of-Things Network Based on User Participation” (Ljungblad, 2019). Therefore this section will be more focused on the aspects of the blockchain used by the mobile application.
The most significant part of the blockchain in this solution is the smart contract. The smart contract handles the data on the blockchain network and confirms or denies incoming transactions. The smart contract also describes how the data is structured on the blockchain using an Application binary interface (ABI). The ABI is built into the mobile application which makes it possible to communicate with the blockchain using the smart contract. There are two functions in the smart contract used by the mobile application. These are “getBalance” and “updateThing” and show in figures 11 and 12 below. The “getBalance” function returns the balance of the given address, which in this case is the users address on the blockchain network. The users balance is the amount of bonus points the user has which is implemented for a future bonus system to give users an incentive to use the application. These bonus points can only be changed by functions on the smart contract.

The second function is the “updateThing” function which is given 3 inputs from the mobile application, as mentioned earlier these are the MAC-address of a Ruuvi-tag, the temperature given by the Ruuvi-tag and the timestamp of when the mobile application received the data. The function saves this data and gives the user 10 bonus points.

```solidity
// Returns the balance of address "a"
function getBalance(address a) public view returns (uint256) {
    return balanceOf[a];
}

Figure 11: getBalance function in the smart contract

function updateThing(string memory _id, int256 _value, string _timestamp) public {
    // Update data
    things[_id].id = _id;
    things[_id].value = _value;
    things[_id].timestamp = _timestamp;

    // Emit event for historical data regardless
    emit UpdateThing(_id, _value, _timestamp, msg.sender);

    // Get reward for uploading data
    _addBalance(msg.sender, 10);
}

Figure 12: updateThing function in the smart contract
4.2.4 Decentralized Application

The Decentralized application is a web page which shows the data saved on the blockchain network. The Decentralized application can view the data saved by using the ABI of the smart contract.

4.3 Limitations

During the design phase and the implementation phase some limitations appeared due to time constraints and due to not being in line with the focus of this thesis. These limitations are described below.

One limitation discussed during the design phase was that the mobile device will not collect or send data automatically in this solution, even if it is planned for a future solution. This is because a manual solution is faster to implement and simplifies testing of the system. Since the solution can be tested with a manual system, implementing an automatic system would take time off the focus of this thesis.

Another limitation discussed during the implementation phase was to not configure the Ruuvi-tag to specifically fit the planned Luleå Kommun case. This choice was made because of time constraints. Instead of configuring the what data sent by the Ruuvi-tag, the type of data already given from the Ruuvi tag is used. With this data the solution could still be tested since the type of values wanted from the sensor already was given by the Ruuvi-tag. As mentioned earlier in the design section the needed values from the sensor was:

- Some sort of identification (ID number or MAC-address)
- Data-Value (The information we want to access in the solution)
- A timestamp of the time when the data is sent

These types of data is given by the Ruuvi-tags given weather sensor system. The Ruuvi-tags are identified by using MAC-addresses, The data values used for testing is the temperature given by the weather sensor. The only type of value not given by the Ruuvi-tag was the timestamp, this was solved by the mobile application saving a timestamp of when the information was received.

The last limitation in our solution is a problem that couldn’t be solved during the timeframe of the project. That problem is a connection problem between the blockchain and the mobile application. The mobile application can't connect to the private blockchain network, instead the mobile needs to be added to the blockchain network manually from a computer by using the IP-address and port-number of the phone. This problem needs to be solved if the solution is going to work in a real life situation. Even if this problem exists it is still possible to connect to the blockchain, manually that is, which makes it possible to test the solution.
5. Discussion

In this section the final solution will be discussed and analyzed, compared with the earlier knowledge given in this thesis and other solutions of IoT networks, blockchain networks and security implementations. This will firstly be done by comparing the solution to the CIA triad which will be a good indication if a blockchain network could help maintain the information security in an IoT network of this type, and propose possible improvements to ensure the information security that was not covered by the blockchain technology. This section will be finalized with an analysis of the bonus system implemented from an information security perspective as well as the list of important aspects described in section 4.1.1.

5.1 Confidentiality:

Since confidentiality as mentioned earlier states that only authorised users should have the possibility to access the information on the network, there occurs a problem when storing the information on a blockchain network. This is because of what many see as a benefit of blockchains, that everyone can access the information on the blockchain. These two different concepts completely contradict each other. Therefore there needs to be another way to achieve confidentiality when creating a system with the use of a blockchain network. Since this solution makes use of smart contracts a custom ABI is generated to assist the users with decoding the smart contract and the information the smart contract holds, which is stored on the blockchain as bytecode. People without access to the ABI will not be able to understand the information stored on the smart contract. The ABI however is not intended as an encryption service and attackers can therefore still access the information and try to find out the ABI by testing their way forward, which can be hard but possible.

A big reason for confidentiality to be so important in a network with a large number of users is because of the users personal integrity. This is handled really well by blockchain since it does not need to store any personal information on the blockchain. The only “personal” information required in a blockchain or distributed ledger network is the users unique cryptographic signature.

A possible solution to this problem is by implementing an encryption service such as the public key infrastructure described earlier in this thesis. A properly implemented PKI can keep the information on the network confidential and only accessible by the users that is supposed to access the information. Where the certificate authority is handled on the blockchain instead of being a third-party organization. Therefore solving the criteria of the Confidentiality concept of the CIA-triad.
5.2 Integrity:

Integrity in the CIA-triad states that the information must be trusted and will not be tampered with during transit or when stored on the network. The blockchain technology solves one part of this, when the data stored on a distributed ledger or blockchain will not be changed, it is at least nearly impossible to change the data that is stored and will get harder when there are more users on the blockchain. The major Integrity problem that occurs designing an IoT network of this kind is therefore while the information is in transit, before the information is written to the blockchain. Therefore solutions is needed to secure the right information is written to the blockchain and avoid threats such as the information being tampered with before written to the blockchain and people claiming to be someone else (i.e a sensor).

There are a few possible solutions to ensure the integrity of the information in a network of this kind. The first possible solution is the same solution given to solve the confidentiality problems of a blockchain network, and that is implementing a PKI. A properly implemented PKI could make the system trust each other since its all encrypted and signed by the senders. For example the sensors could sign and encrypt the information before sending the information to the nearby mobile phones, which leads to the users knowing if the information given can be trusted or not.

Other possible solution to confirm that the correct information is written to the blockchain are either finding or developing a new consensus method more suitable for this solution, Since proof of work does not control if the information gives is correct and only controls if the block has an acceptable hash value. Or implementing a method in the smart contract that requires other users confirm the information given by one user before its written to the blockchain. For example a user sends a transaction to the smart contract which triggers a method which requires a small amount of users to send the same data value from the same sensor during a certain time period, to be approved. These kind of methods will have to be designed with the solution in mind. Since the data values can be different depending on the use case of the system. For example in this solution implemented, the data value is the temperature given from the Ruuvi-tag and a temperature value is unstable with small changes occurring throughout.
5.3 Availability:

Since availability as mentioned earlier states that the services of the network should always be available, such as the systems used to store and process the information. Since the blockchain technology is peer-to-peer, services should be available as long as a peer is active, which shouldn't be a problem in a large scale solution, as well as removing the need for a third party making the network neutral. This is especially true if the solution is implemented in a public blockchain network instead of a private ethereum network as the solution created in this project. When connected to a public blockchain network there should always be a peer connected making the services available. Even if blockchains solves the availability problems that can occur in an IoT network, there still is two availability problems in this solution. These problems are when mobile users don't have an internet connection and will not be able to send their information to the blockchain and when a person steals one of the sensors making the sensor not available in the network.

It may not be worth putting additional resources to prevent theft of the sensors, therefore its better to take precautionary measures such as not using too expensive hardware and instead using smaller relatively cheap hardware (i.e Ruuvi-tags).

To solve the problem of users not having internet connection making some services of the system available while offline. A solution would be to implement a buffer that temporarily stores the information until the user has internet access and when the users gains access to the internet the information should be sent automatically. This is not how the solution works at the moment since there is no automatic scanning/sending of transactions implemented. Because of the connection problems mentioned in section 4.3 there is currently no implemented solution for the mobile user to see if the connection to the blockchain is lost or still active after it is first established, this needs to be solved in the future.
5.4 Bonus system

One part this project was to create a user incentive for the user participation by using a bonus system, while keeping the personal information about the user secure. This system works by storing a “currency” on the blockchain connected to the users cryptographic signature. This currency is controlled by the smart contract and in the current solution there is no implemented method to use this currency. In a future optimal solution the users should need to send a transaction to the blockchain to use the currency, that transaction will be signed by the user by logging in on its account by using the digital signature and the password which only the user knows. Looking at this system form an information security perspective. There is no personal information stored and accessible by others, the amount of currency is stored on the blockchain and will only be changed by the user sending transactions to the smart contract meaning the integrity of the bonus system is ideal. The biggest problem of this system is on the availability side of the CIA-triad where the user will need an internet connection to access and use the bonus points.

5.5 Important aspects

To analyze the system further, the solution is compared to the list of important aspects described in section 4.1.1. This is done to get a better understanding of where blockchains can provide solutions and where other future work is needed. The content of the list of important aspects is analyzed in the subsections below according to the categories given in the list.

5.5.1 Availability

- Data and services should always be available. Network communication and application availability should have as high uptime as possible.
- The network should not rely on a third party to be maintained. The removal of the need of a third party makes the network neutral and available to several different actors.

As described in section 5.3 a blockchain network provides solutions for the availability of a system. This is mainly because of blockchains networks being peer-to-peer making the services available as long as a peer is active as well. Blockchain networks being peer-to-peer also removes the need for a third party handling the data making the network neutral.
5.5.2 Communication

- The network has to be delay-tolerant because it cannot support real time updates due to the fact that it relies on humans to pass by the sensors and collect the data.

This system is currently in different ways delay tolerant, where the Ethereum blockchain is delay tolerant. As well as the implemented and the Luleå Kommun use case would not require real time updates so function.

5.5.3 Cost

- It should be free to participate in the network.
- Sensors should be cheap. Preferably less than 20 euro per unit.

The goal of having a completely free network is unfortunately not reached. An Ethereum blockchain network does not allow the user to send transactions without using a type of currency called gas. To solve this problem a solution could be to explore other options to the ethereum blockchains such as other types of blockchains of distributed ledgers.

The ruuvi-tag used is this solution is almost meets the requirements of being a relatively cheap sensor where the cost is between 20-30.

5.5.4 Incentive

- Any kind of participation should be rewarded to create a win-win situation for all users
- Data collectors are rewarded with bonus points which can be redeemed for items or services, for example discounts.
- Sensor owners are rewarded with collected sensor data.
- Sensor owners get access to a relatively cheap communication network.

In this solution a win-win situation is created, where the sensor owners get access to a relatively cheap communication network, are rewarded with collected sensor data and the data collectors are rewarded with bonus points. However there is currently no implemented way to use the bonus points, but the foundation is there.

5.5.5 Maintenance

- Sensor battery life should be long. Preferably longer than 1 year.

The ruuvi-tag used is this solution is meets the requirements of having long battery life with a battery life longer than 1 year.
5.5.6 Security

- Data should be tamper-proof.
- Users should be able to trust that other users are who they say they are.
- Wireless communication should be encrypted.
- User integrity should not be compromised.

As described in section 5.2 a blockchain network can provide integrity over the data stored on the network. The data stored will be tamper proof and the users are trustworthy using their cryptographic signature, which is the only information stored about the user making them anonymous and therefore securing the users integrity as well. However due to time constraints an optimal solution to encrypt the wireless communication is not implemented and future work on encryption is required for a final solution.

5.5.7 Usability

- Both applications and smart contracts should be open source.
- For data collectors: application that displays their information such as account address and bonus points.
- For sensor owners: application that displays collected sensor data.
- Mobile application energy consumption should be low to not affect mobile phone battery life.
- Mobile application memory storage requirement should be low to not fill mobile phone memory.
- New users should always be allowed to join the network.

New users will always be allowed to join the network. The mobile application can display information such as bonus points to the users, as well as managing being connected to the blockchain without affecting the mobile phone’s battery life of memory. However the mobile is not currently uploaded and therefore is not open source. The data collected can be viewed by sensor owners on a distributed application.
6. Conclusion

When looking at the current solution compared to the CIA-triad, there is definitely benefits when using blockchains in an IoT network of this type. The experience and knowledge gained from researching and implementing this solution to create an understanding on how blockchain technology can support the communication and security in an Internet of Things network. Leads us back to the starting problem statement: How do you maintain the information security in an Internet of Things network based on blockchains and user participation?

The blockchain technology offers plenty of solutions to information security problems that can occur in IoT networks, especially within the integrity of the information and the availability of the services since blockchains is peer-to-peer. The biggest problem is within confidentiality where all the information on the blockchain can be accessed by everyone which makes this not a suitable solution for a system were sensitive or classified information is stored, because even if we encrypt the information with a really secure encryption method the encryption could still be solved in theory. However the Luleå Kommun case described in this thesis does not use any classified information therefore making blockchains a suitable solution.

Since the blockchain technology only stores and manages the information there are still some problems that occurs in every IoT network, such as trust issues. Even if the information on the blockchain is secure and can be trusted it doesn't cover the part of the solution when the information isn't stored on the blockchain. Therefore an encryption service for the wireless communication such as the public key infrastructure is needed to maintain the information security in the network.

When generating a bonus system to create a user incentive the blockchain technology creates an ideal security for the bonus system since the user is anonymous and the users currency will only be changed by the smart contract. Where the only major problem is that the bonus system isn't available without an internet connection.

This thesis has provided an understanding about other uses of the blockchain technology compared to the more common uses such as a cryptocurrency. This new knowledge can hopefully provide help for future research regarding information security when using blockchains or distributed ledgers in internet of things networks.
References

Books and papers


Websites
