Faculty of Technology and Society

Department of Computer Science

Spring 2016

On the application areas of blockchain

By

Zahra Ghaffari

Zahra.Ghaffari@mah.se

Supervisor: Bo Peterson

Examiner: Radu Mihailescu

Contact information

Author: Zahra Ghaffari
E-mail: Zahra.Ghaffari@mah.se
Malmö University, Department of Computer Science

Supervisor: Bo Peterson
E-mail: Bo.Peterson@mah.se
Malmö University, Department of Media Technology and Product Development

Examiner: Radu Mihailescu
E-mail: Radu.C.Mihailescu@mah.se
Malmö University, Department of Computer Science

Abstract

The goal of this study is to identify the current application areas and some possible application areas for blockchain; blockchain is a distributed database that is currently most known for being the technology used for storing transaction information of digital currencies such as the Bitcoin. Through a literature review and interviews with domain experts, we identified some current application areas for blockchain, that is, money transactions, decentralized data and privacy protection, and decentralized autonomous organizations (DAO). Within the area of decentralized data and privacy protection, we further identified the two sub-areas of smart contracts and secure identities. In addition, we identified some possible application areas by conducting a second literature review. Some of these application areas are: storing mind files and human intelligence, on-line voting, supply chain management, stock trading, Internet of Things (IoT), and banking. The contribution of this study can be used for further studies through each of the above application areas in order to identify possible advantages and disadvantages.

Keywords: Blockchain, Bitcoin, cryptocurrency, decentralized privacy, application area, data protection, secure identity, smart contract, decentralized autonomous organization, DAO, Internet of Things, IoT

Acknowledgement

This Master's thesis was performed as part of fulfilling the requirements of a Master's degree in Computer science at Malmö University.

I would like to express my gratitude to my supervisor Bo Peterson for introducing me to the topic and for his useful comments and engagement during my work with this thesis.

I would like to thank Martin Dalsenius and his colleagues Martin and Jonas from the company Bit4m for participating in two interviews and for contributing with their knowledge and good discussions.

I would like to thank my life partner Johan Holmgren; having his love and support helped me throughout the entire process by keeping me harmonious and giving me inspiration and motivation to complete this thesis. I would also like to thank my family, especially my children Nina and Benjamin for being supportive and understanding during this time.

Last but not the least, I would like to thank Malmö University and the Department of Computer science for supporting me to finish my Master's thesis.

Table of content

1. Introduction

1.1. Project idea and goals

The possibility for two parts to transfer money over the Internet without a trusty third party has been a challenge for several years. The vision of safe digital currency transactions was realized through the introduction of the Bitcoin currency in 2008.

The foundation of the Bitcoin currency is a peer-to-peer network of computing nodes. These nodes cooperate in order to ensure safe transaction; however, due to mechanisms built into the system, there are no incentives for the nodes to cooperate in order to attack the network. In addition, computers may leave the network whenever they want, and they are allowed to join the network by their own choice if they accept the longest chain of proof of work, which was built when they were gone. The Bitcoin network is based on a proof of work protocol and built by time stamped transactions that are hashed together to a long chain of transactions. [1]

Blockchain, which is the main technology behind the Bitcoin currency, is a public shared ledger that stores the information that it provides from the different parts involved in the transactions that are done in the entire Bitcoin network. In particular, the Bitcoin network uses the blockchain to store the history of the transactions and all the information about the transactions [2], such as the time when the transaction took apart, the address of the sender (or spender) of money, and the address of the receiver of money. This will help the spenders to avoid double spending their money. All the information is encrypted in order to protect the integrity of the blockchain [4]. Since the blockchain stores all the information about all the Bitcoin transactions [1], the blockchain can also be described as a decentralized database [16,26,36]. For a complete description of the blockchain model, we refer the reader to Tewari and Noallain [7].

Following the Bitcoin currency, other digital currencies have later on emerged, such as, Namecoin [5] and Certcoin [6], which also build on the same technology (blockchain) as the Bitcoin currency. Other than digital currencies, there are very few known application areas of the blockchain, despite the fact that it has successfully provided strong secure digital currencies that is widely used. For example, according to coindesk.com[1], the number of daily Bitcoin transactions has increased to about 200.000.

Due to the recent success of the blockchain, as the main technology behind the digital currencies like Bitcoin, we find it relevant to identify other application areas of the blockchain technology. According to the best of our knowledge, there exist no structured overview of the current and potential applications of the blockchain, and the main purpose of the current work is to provide such an overview.

As mentioned above, an important purpose of the current work is to identify different application areas that currently use blockchain. Another purpose of our work is to identify potential future application areas for blockchain.

1.2. Research questions

As mentioned in the previous section, the main purposes of this work are to identify 1) the current application areas of the blockchain and 2) the possible application areas of the blockchain.

The purposes are captured within the following two research questions:

[1] http://www.coindesk.com/data/bitcoin-daily-transactions/

- RQ1. What are the current application areas of the blockchain?
- RQ2. What are the possible application areas of the blockchain?

It should be noted that RQ1 is completely answerable by studying the current research literature. We have chosen to formulate RQ2 in way that it can be only partially answerable. The degree to which it can be answered depends on the current knowledge on possible application areas. However, we have chosen to include it due the fact that it very well captures the second purpose of this thesis.

1.3. Limitations

The blockchain technology began with the Bitcoin crypto currency [1] in 2008. It is an issue that this new and young technology just began being used for different areas and it is still in testing stages for many application areas such as banking [20]. The limitation is that there are not many academic works in this manner being done.

2. Research method

In this work, we used the three methods that are shown in Table 1, that is, literature review, searching on the Internet, and interviews with domain experts.

Table 1. A mapping between our research questions and research methods

Research methods	RQ1	RQ2
Literature review	X	X
Online searching	X	X
Interview	X	X

2.1. Literature review

In this work, we adopted a qualitative research approach, where the main method is the literature review using a systematic approach. In particular, we gathered the data needed in order to answer our research questions by analyzing articles related to the blockchain.

For RQ1 (What are the current application areas of the blockchain?) we used a traditional literature review with a systematic approach where we searched for application areas in relevant databases. We started our searches using the following keywords and phrases, which we identified as highly relevant.

- "blockchain"
- "block chain"
- "block chain" + "application area",
- "blockchain" + "application area",
- "bitcoin".

Based on the results from the initial searches, we refined the search phrases, for example, by adding more keywords. We limited our searches to the databases *ACM Digital Library*, *Google Scholar*, *Science Direct,* and *IEEE Explore* to find the relevant articles for our topic. In addition, we focused on articles published year 2008 or later than the year that the blockchain was introduced by Nakamato [1] together with the Bitcoin currency.

By finding the similarities and differences in the application areas that are currently using blockchain, in the next step of our research we tried to draw conclusions about possible applications areas (of the blockchain).

We further analyzed the identified application areas, that is, the answer to our research questions, in order to identify their main characteristics. We also analyzed the blockchain in order to identify its key characteristics, that is, the characteristics that made it applicable for the identified application areas. The outcome from this analysis served to help us understand the structure of the blockchain and the usage of it in general.

In the final phase of our project, we approached RQ2 (What are the possible application areas of the blockchain?). In this part we defined keywords and search phrases based on the outcome of the first

literature review. That is, the identified characteristics of the blockchain and its current application areas were the basis for the search phrases in the second literature review. The outcome of the second literature review was, obviously, a set of relevant application areas for the blockchain.

2.2. Interviews with experts

Another way to gather the data about application areas of the blockchain was to conduct interviews with experts who are currently working with the blockchain. The purpose of such an approach was to help us getting relevant information from experienced experts in the area. We conducted two interviews to gather data to help answer our two research questions and evaluate the results. We conducted our interviews according to the recommendations of Creswell [3], who described how to conduct face-to-face interviews in order to elicit the opinions from the interviewees.

2.2.1. Interview guide

An interview guide is a plan for scientists to proceed to find respondents, design questions, conduct the interview and analyze the data that the interview produces [27]. Our interview guide was designed with two parts: general questions and specific questions. The general questions part contained seven questions and the specific questions part contained three questions. The questions were designed as Creswell [3] described to be open for follow up questions and to give the expert opportunity to reply to the questions, which can give us a larger amount of, and possibly more detailed, data. The outcome of the interviews helped us understand the purpose of using blockchain for the company and to collect the main characteristics of blockchain from the expert's point of view.

2.3. Online searching

As a complement to using the scientific literature we conducted an online search to gather information from online magazines and some other up-to-date information sites. This approach gave us the opportunity to obtain the latest news of what is currently happening within the field of study. Since the blockchain is a quit new technology, new news and findings in the area are constantly published. There are simply not so many research articles about the new findings that happened recently, which is the reason and the motivation for the importance of using online searching as a research method in this study.

2.4. Alternative methods

Another possible research method to approach our research questions would be to design a questionnaire, which we could send to professionals who are currently working with blockchain technique. Such a questionnaire could be analyzed in order to understand these people's views on the current usages of the blockchain and on their opinions about other possible application areas. According to Creswell [3], this is a quantitative research approach. We consider this approach to be not viable since these persons most probably are difficult to identify.

3. State-of-the-art

In the literature review described below, we identified two areas of application of the blockchain, that is *digital crypto currencies*, and *decentralized privacy and data protection*. Since our project focuses on the current and possible application areas of the blockchain, both of these application areas are related to the research questions of our project.

3.1. Digital crypto currencies

In this subsection, we summarize some of the work that has been carried out within the digital crypto currency application area of the blockchain.

Nakamato [1] announced in 2008 that they identified a solution for the e-money problem, which is recognized as an expensive and difficult issue when doing money transactions over the Internet. Traditionally, transactions have been difficult to protect due to the need for a trustworthy third part in between the sender and receiver of money. However, it can be difficult to find third parties that can actually trusted. In addition, the third party always costs money.

A solution to the e-money problem is the software Bitcoin, which is based on a (peer-to-peer) proof of work network, where the two parts involved in a transaction are both members. A user of this network uses a private key to prove his/her right to use bitcoins from a wallet through another signature that is cryptographic. This signature protects the owner from double spending bitcoins, or to get the wallet or identity stolen. All of the transactions are protected from change as described next. Each transaction is added to a block that is a record over the most recent kept and confirmed transactions. The first block is called the genesis block. After approximately ten minutes, a new block is created and joined to the blockchain. The blocks in the blockchain are completely unchangeable because of their structure. If the information about the transactions in the blocks changes, all the following blocks will be corrupted and invalid, which leads to an infeasible blockchain. The blocks make up a chain called the blockchain, which is shared among all the Bitcoin wallet users. In addition, it is considered completely safe from every outside attempt to change the blockchain. The blockchain makes it possible to record a transaction chronologically and protect it from revoking. The blockchain protects the Bitcoin users from double spending their money, since every transaction must be confirmed before sending and registration [1,4].

Namecoin is another crypto currency that is based on the Bitcoin's blockchain with some modification in the blockchain. The Bitcoin's blockchain stores the information about the money transactions that give Bitcoin an identity to be a monetary-value store, while Namecoin's blockchain also stores DNS information. In addition, the Namecoin's blockchain is also able to store the identification and authorization database. Just like Bitcoins, Namecoins is vulnerable to name stealing; it is very difficult to steal the names but when it happens it is usually difficult to recover from the damage. [5]

Fromknecht et al. [6] contribute yet another crypto currency called Certcoin, which is based on Bitcoin and Namecoin, but it does not allow two users having the same name identity. This feature is managed by using name dictionary data structures in the blockchain in order to protect the identity of the current users. In their work, they use hash table distributed public key lookup. The process of the lookup, which generates a public key that can be used to enter the network, uses a user identity together with a public key. To check for a name in the blockchain, the user has to go through the whole blockchain and control if there is an active registration in order to get a key generated from the registration and all the updates. The user does not need to control all the signatures for the updates, since the signatures have been already controlled when the registration was initially added to the blockchain.

Another electronic payment system is Netcoin, developed by Tewari and Nuallain [7] in 2015. Netcoin is similar to Bitcoin; however, with some differences in order to take the control over the growing public ledger in the blockchain. Netcoin applies a blockchain that stores the transaction history of each coin, which means that each coin in the system has a unique identity. This enables to spend a coin more than once while this option is not applicable in Bitcoin. Another contribution of Tewari and Nuallain, is that Netcoin prevents wasting a lot of computing power by letting the network verify the legitimacy of each coin and its user instead of using a proof-of-work strategy which is used in the Bitcoin system. However, as soon as the length of a coin's blockchain is close to a certain threshold, there will be a re-issue of the coin to the current owner of that coin in order to prevent large storage and bandwidth problems as a consequence of a long blockchain.

3.2. Decentralized privacy and data protection

In this subsection we present another application area of blockchain, which we refer to as decentralized privacy and data protection.

One of the applications that provide user data protection and privacy protection is the one that Lazarovich [8] develops. Lazarovich develops a platform similar to the Bitcoin's blockchain with the purpose of protecting and storing sensitive data. This platform is also decentralized and can be used by real applications for different service providers. Lazarovich also evaluate the platform and test it for the above purpose. The contribution is a platform to protect privacy and personal data, which is applicable for many different applications where the user is unable to protect his/her own personal data and instead has to rely on a trusted third party. Lazarovich develops two mobile applications and a web dashboard. Examples of other applications that can count into this category are Facebook, health care, and AirBnB [8].

Hawk is a smart contract system that Van Den Hoff et al. [9] present in order to make transactions and contract systems in decentralized digital currency systems publicly visible. This might be useful, for example, in order to prevent money laundering. The people using the system do not have to encrypt the private information about transactions, since it will get a cryptographic protocol from the compiler that is used. The interaction with the blockchain is the same as in Bitcoin, except the cryptographic private information that is not available for others (in Hawk). Hawk is designed in such a way that it can be used also for digital transactions.

Zyskind et al. [10] suggest a decentralized privacy system, which makes use of the Bitcoin blockchain in order to protect personal data. In order to make this kind of protection possible, they use blockchain as a database that stores personal data. The user enters his/her data in the blockchain, and the companies and authorities, which need to access the information, can use it without having any responsibilities about storing the private information. Users do not need to trust a third party and always get the information about how and what their personal data is used for. This aim is made possible by using a blockchain as a control moderator combined with other types of storage solutions. The solution gives the opportunity for the user to take control over his/her private information and prevents the data from spreading out.

4. Results and analysis

4.1. The process

The outcome of the three methods that are presented in Chapter 2 helped us to answer our two research questions. The implementation of these methods is presented in the three upcoming sections (4.1.1-4.1.3).

4.1.1. Interviews with experts

We conducted two interviews with experts from the company Bit4m [35]. Bit4m is currently working with money transactions across several countries. The vision of Bit4m, as they expressed in the two interviews, is to make an application for money transactions, which can be used globally. Their application can be compared with Swish [46], which is an application used for money transactions nationally. Transferring of money by Swish is done through the use of the receiver's mobile phone number. The simplicity of this service is that the application uses another application named *Mobile bank id*. Mobile bank id is an application, which is used for personal identification. As the sender opens the Swish app on the smart phone, the app redirects the user to the app Mobile bank id. As the user correctly logs in to Mobile bank id, it will be possible to transfer money to a receiver by using the receiver's mobile phone number.

The aim of the Bit4m application [35] is to offer an application to transfer money similar to the way Swish works, which can be used for international money transactions. Bit4m already has this service for some countries, and they are working across different countries for offering this solution in some other countries.

The Bit4m application is based on the Bitcoin's blockchain in the middle, and it has traditional currencies in both ends. For example, this solution makes it possible to send Swedish currencies (crowns) to the USA to receive the amount of sent money in US dollars. The solution is very fast, effective, and secure.

The aim of conducting the first interview was to gather data for the results. The aim of the second interview was to evaluate the obtained results.

We present the interview questions for the first interview and second interviews in Appendix A and Appendix B, respectively. In order to avoid confusion and misunderstanding, we present the results of the two interviews separately. The summaries of the questions from the second interview are presented in Section 5, since the aim of this interview was on the evaluation of the acquired results. The summaries of the answers to the questions from the first interview, in order to answer our research questions, are presented below.

1. *What are the main characteristics of the blockchain?* Blockchain is a distributed database that makes it possible for all the users in the network to have access to a safe, fast, and effective solution. The main characteristics are transparency, fastness and effectiveness.

2. *What are the strengths of the blockchain?* It is very safe, easy to verify, and transparent. The blockchain is a faster way to processing the data.

3. *What are the weaknesses of the blockchain?* The blockchain demands a lot of CPU capacity for computing. It is consciously built to be difficult for computations, and it demands a lot of energy.

4. *What do you believe about the progress of blockchain in the future?* Blockchain is going to be more and more important for different types of applications when it comes to who owns what, since the data stored in blockchain is difficult to manipulate but easy to access.

5. *Why did you choose blockchain for your solution?* From the beginning we wanted a solution like Swish, but globally, and we believe that this will happen.

4.1.2. First literature review

After conducting our first literature review, when we searched in the four databases *ACM Digital Library*, *Google Scholar*, *Science Direct,* and *IEEE Explore* with some relevant keywords and phrases, we found some relevant articles and websites to study and use in this work.

4.1.3. Second literature review

The second literature review was based on the material we collected in the first literature review. In particular, from the first literature review we identified a number of researchers that were active in the area, and we searched on these researchers' websites for updated research. We used this outcome and searched for further literature in the two databases *ACM Digital Library* and *Google Scholar*. The outcome of the second literature review and the results from the Internet sources helped us mainly to answer the RQ2.

4.1.4. Online searching

As a complement to using the scientific literature we identified information in some online magazines and some other up-to-date information sites in order to get the latest news about what is happening in the field. As a basis for our online (Internet) searches, we used the keywords that we identified in the first literature review (see Chapter 4.1.2).

After we completed the analysis part, we identified the main characteristics of the current application areas and mapped these to the main characteristics of blockchain (see Table 2).

Table 2. Mapping between the current application areas of blockchain and the main characteristics of blockchain.

Application area	Characteristics			
Money transactions	Transparency	Faster to handle the data	Cheap	Easy to access the data
Smart contracts	Transparency			
Secure identity		Faster to handle the data	Cheap	Easy to access the data
DAO	Transparency		Cheap	Easy to access the data

We identified the above characteristics and searched for phrases that contain two or more of the characteristics (in Table 2) and the application areas. In the next step we searched for these relevant phrases on the Internet. From these searches we identified some additional information sources and additional relevant information on the blockchain.

4.2. Answer to RQ1

When presenting the result for the RQ1, we divide this part into three parts representing the following application areas:

- Money transactions
- Decentralized privacy and data protection
    - Smart contract
    - Secure identity
- Decentralized Autonomous Organizations (DAO)

4.2.1. Money transactions

Blockchain has been used as the main technology in digital currency transactions since 2008, when the Bitcoin currency [1] was introduced but it can merge to be much more according to Swan [23]. Swan [23] states that blockchain is going to become the next computing paradigm after mainframes, PCs, the Internet and mobile social networking.

As shown in Figure 1, the blockchain works as a transparent puzzle, where each piece of the puzzle is a transaction history from a sender A to a receiver B, which has been approved by all the members of the network. [11]

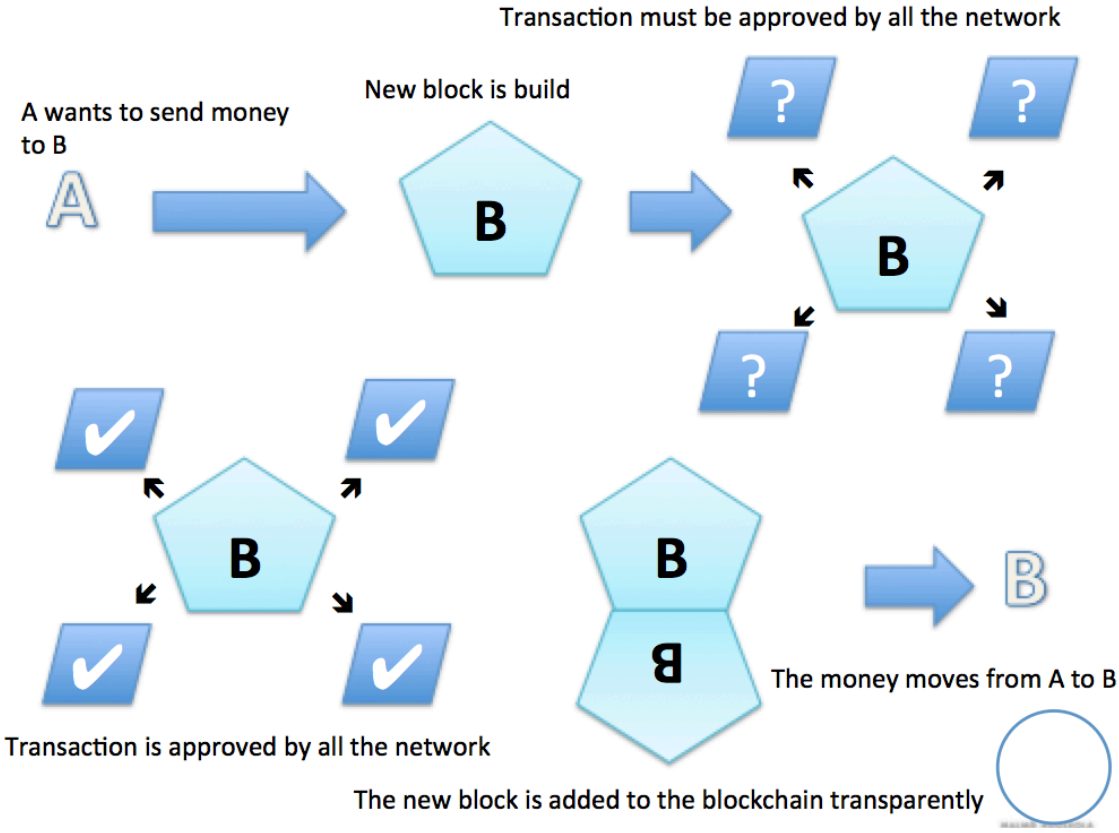

Figure 1. An illustration of how blockchain works in a transaction from A to B.

According to the coin Market Cap [15], which is an Internet site listing digital currencies, there were, by April 2016, 730 digital currencies in the digital world.

Certcoin is a digital currency that is very similar to Bitcoin and Namecoin, which use the same technology; however, it uses the real PKI (Public key Infrastructure). The difference between Certcoin

and Bitcoin is how they identify their users. Certcoin is based on, and builds on top of the Namecoin currency. [6]

In September 2015, nine of the biggest global banks started to cooperate together in order to test the technology of blockchain. The aim of this cooperation is to achieve three different goals. The first goal is to develop a platform to handle the huge amount of money that is being used in the financial industry. The second goal is to experiment with the new tool (i.e., the blockchain) in order to understand how it works. The third goal is to build new useful tools that can be applied in the financial industry [29]. In addition, in February 2016, DiGITAL [17] wrote that 2 of the biggest Swedish banks began cooperating with 22 other banks in a project to work with blockchain technology. Moreover, in April 2016, Reuters [18] announced that the Swedish bank *Nordea*, the Japanese bank *Mizuho Bank,* and the Italian bank *Unicredit* initiated a blockchain-cooperation with the startup New York based company *R3* in order to build a framework for using blockchain in their transactions. BBC [45] announced that eleven banks tested trading solutions based on blockchain in January 2016. According to CNBC [21], *The Barclays*, *UBS*, *UBSG.VX*, and *HSBC* are some of the large banks involved in this project. The aim of this collaboration is to find out how these banks can use the blockchain in the financial world. These tests are applied using the Etherum [20] instead of Bitcoin.

Bitcoin is used to make change tipping easier on the Internet. For further information we refer to changetip.com [14].

Etherum [32] is a blockchain based transaction ledger that is decentralized and can be used in transaction of different types of services, for example, digital currencies. Etherum can also be used in smart contracts.

4.2.2. Decentralized privacy and data protection

Another application area for the blockchain is to use blockchain in order to achieve decentralized privacy and data protection. There are in particular two identified application areas in this manner, smart contract and secure identity, which we describe in Sections 4.2.2.1 and 4.2.2.2.

In order to explain why blockchain is being used for the decentralized privacy and data protection we below explain briefly the whole process for saving data in the blockchain.

As Nakamato proposed [1], the idea is based on a proof-of-work network where nodes can join freely, but once they attempt to join the network they have to accept the whole blockchain that was built before they joined. By accepting the blockchain they accept the validity of the blockchain. Every node will vote using their CPU power and work on extending the valid blocks and reject the invalid blocks. This will be the reason that the blockchain that is longest is the valid blockchain in the network. [1]

4.2.2.1. Smart contract

A smart contract is a program that makes a contract between two parties completely automatically. Like the Bitcoin, the information about the contract is stored in the blockchain. When something goes wrong with the (smart) contract, the system is automatically locked and enforces the contract to breach without the interference of a third party. [19] The idea was introduced 1994 by Nick Szabo[30].

Kosba et al. [9] contributed one of the first solutions for decentralized smart contract systems by using blockchain and cryptography [12].

Juel et al. [24] announced that they initiate criminal smart contracts to avoid criminal activity that can be caused by transparency. They contributed a new technique to avoid leakage of secrets, key theft, and calling card crimes.

4.2.2.2. Secure Identity

In December 2014, the wall Street Journal [29] announced that the digital personal id by Onename currently manages 24000 user identities. A Onename id is a digital id that can be used in order to identify a person. It is similar to other systems that outsource the identities to a third party; however, the digital id also gives the opportunity to identify a person on different social medias such as Facebook and Twitter. The difference between the traditional social media systems and Onename is how they store the information. The social media companies typically store their information using servers that they control themselves. Onename stores the personal data on the decentralized blockchain, similar to the digital currency blockchain. The users have complete control over their personal data through their encrypted private keys, and no third party can obtain the information about them. The digital id is currently developing and the prediction is that it will be the identification mechanism of the future [13,28].

4.2.3. Decentralized Autonomous Organization (DAO)

The forth application area of the blockchain, which we present in this work in order to answer RQ1 is Decentralized Autonomous Organizations.

Mougayar [33] presented a Decentralized Autonomous Organization (DAO) as an organization that uses the blockchain in order to store different kind of transactions completely autonomously. Once the DAO is up and running, it no longer needs its creator in order to function. Buterin [44] announced that the DAO is built on Etherum, and it makes use of Etherum (ETH) as a token for valuating the transactions [42]. DAO is both end user and worker, and the networks outcome relies on the DAO's workers' activity levels. DAO is used for transportation applications, mesh networks, online storage, and health care applications [37]. Some examples of DAO are La'Zooz [38], which is an application for IoT to coordinate transport by finding available car seats, MaidSafe [39] for crowd sourcing, and Bitnation [40], which is a public notary and OpenGarden which is a chat application without any need for Internet connection [41].

4.3. Answer to RQ2

We used the information extracted from the two literature reviews and our interviews, which is described in 4.1.1 in order to predict some possible application areas for the blockchain.

4.3.1. Internet Of Things (IoT)

IoT is one of the possible application areas for the blockchain. IBM [43] published a white paper in 2015, where they presented different future challenges for IoT. In this article Gibson [43] presented the blockchain as the rescue for the future of IoT when it comes to privacy, lower cost and autonomy. Gibson [43] presented the blockchain as "the revolutionary transaction processing tool" for this purpose. Furthermore, Gibson sees the blockchain as a framework to achieve an easier interaction between interacting devices, and he describes his vision as below:

"In our vision of a decentralized IoT, the blockchain is the framework facilitating transaction processing and coordination among interacting devices. Each manages its own roles and behavior, resulting in an 'Internet of Decentralized, Autonomous Things' – and thus the democratization of the digital world." [43]

In addition, Gibson [43] described the blockchain as the universal digital ledger that facilitates different kinds of transactions between devices, such as registration of a new device, authentication of

remote users and contact for exchange with other devices. For the manufacturers, the IoT based blockchain is attractive due to the decentralized nature of the blockchain. Another aspect is that users take control over their privacy without needing a trustful third party. Further, Gibson suggested that in this new model, the cloud would be a peer service provider instead of a manager.

4.3.2. Some other possible application areas

Other possible application areas of the blockchain are all the solutions that keep track of who owns what (see Table 3). These application areas include banking and bank papers, rental companies, stock trading, equity trading, and insurers. [20]

Another possible application area that is currently being tested by *The Barclays* is online voting, which might be more efficient, faster, and safer than traditional voting, as it can be protected from manipulation. Another area is supply chain management. [21]

Swan [22] suggested that the blockchain could be used to store the intelligence of the human brain. In particular, Swan believes that the blockchain can be applied for personal thinking. She further suggests that: "The concept is "blockchain technology + in vivo personal connectome" to encode all of a person's thinking and make it useful in a standardized compressed data format" [22]. The purpose of this would be to store personal memory in blockchain and use it for future decision-making.

Another application could be to store personal contracts when young and healthy. These contracts can be useful in case of sickness if the memory is not in a very good condition. Swan [22] hopes that digital mind files will enhance the digital societies by increasing the intelligence.

Furthermore, the wall street journal [28] recently published an announcement from the founder of Onename: "One day, suggests Mr. Ali, you could use your Onename ID to assign rights and powers to do all sorts of things — "to open your garage door, release your medical records or lodge an online vote."

5. Evaluation of results

We argue that our results to a large extent are already evaluated since we have obtained them by reviewing existing peer-reviewed literature. We have also obtained information from online magazines, which is why we also conducted an interview with a company working with the blockchain.

In order to further evaluate our results, we conducted a group interview with two representatives of the company Bit4m [35], which we already interviewed in the early stage of our research (see above). In order to identify lacks in our findings and results, we designed interview questions to help us with the evaluation of the results. We designed an interview guide, consisting of a set of open questions, based on our obtained results. The interview guide is presented in Appendix B.

In the interview, we chose to explicitly ask for opinions about those application areas that we found particularly controversial, and most interesting, that is, supply chain management, mind files and secure identity. A minor limitation of our evaluation (due to limited interview time) is that we did not explicitly ask about all of the possible application areas.

Both of the interviewees verified our results. Summaries of the answers to the most important questions are presented below.

Verification of the answers to RQ1

1. Which application areas do you know that currently use the blockchain?
   Answer: Juridical contracts that make sure who owns what, money transactions, identification applications and voting.

2. Do you know any companies working within the application areas that you mentioned?
   Answer: Yes, there is a company in Malmö that is working with a future solution for voting.

Verification of the answers to RQ2

3. Which application areas do you suggest can possibly use blockchain?
   Answer: Different kind of trading, stock trading, buys and sell services, and online voting.

4. Do you know any companies working within the application areas that you mentioned?
   Answer: No

6. Conclusions and future work

6.1. Conclusions

Our conclusions are that the blockchain is very useful and applicable in different areas where the solution is demanding safety, transparency, and effectiveness. Mainly, we identified the following current application areas of blockchain, which we present in Section 4.2.1 and 4.2.2: money transactions, decentralized privacy and data protection (smart contracts and secure identities), and decentralized autonomous organizations (DAO). The blockchain is the technology that makes it possible to store information without relying on a trusty third party. BREAKIT [25], a Swedish media website about startups and tech companies, presented some current and possible application areas of the blockchain, such as transaction of digital currencies, contracting, banking, voting, education, rent and selling cars, prognoses, music, networking and IOT, law, car pooling services and stock trading. (See Table 3)

Table 3. Some current and possible application areas of blockchain [25]

Current and possible application areas of the blockchain	
Services and stock trading	**Music**
Car pooling	**Prognoses**
Law	**Rent and selling cars**
Networking	**Education**
IOT	**Voting**
Transaction of digital currencies	**Banking and contracting**

As it was discussed in the previous chapter, blockchain is predicted to be useful for any application area where it is necessary to register who owns what. One example, within the music application area, is that blockchain can be used to store the music from different artists, where each artist is associated to his/her own music and get paid directly using smart contracts. Another example of an application area is car pooling services where the renter is having all the information about the car in the blockchain as a public ledger, and the rentee can sign the contract from the car he/she is renting at the time of rental, and the rental information is automatically stored in the ledger. See [25] for more examples.

In addition, we identified some possible application areas of blockchain, which we present in Section 4.3. One of these, suggested, possible application areas are storing mind files [22] in the blockchain to use in case of illness and loss of mind. These suggestions show the decentralized role of the blockchain in the future. The blockchain might be the answer to the problem of data protection and privacy in IoT as it is decentralized and free from a third party's influence; however, the future will show whether this will be the case. In DAO, the Blockchain is a powerful way to store different information and data from automated devices, which are sending and receiving data to and from each

other in the world of Internet of Things. In IoT, the blockchain has also been predicted to be the universal digital ledger that facilitates different kinds of transactions between devices, such as registration of a new device, authentication of remote users and contact for exchange with other devices [43].

Based on the obtained results we are confident that the usage of the blockchain will grow very fast in the future. Furthermore, the results show that blockchain has a large capacity to be a solution for different problems concerning ownership. We further believe that the blockchain will be used in several application areas for permanent storage of different types of data for future usage, without a trusty third party, in a very effective way.

As the *Business insider UK* [31] announced in December 2015, the New York Startup company R3 got the 42 biggest banks signed into a project to test the blockchain. Currently, when a money transaction takes place, it is necessary for the banks involved to contact each other, which is a process that takes a lot of time. The joining banks hope that the blockchain technology will make this process very fast, cheaper, and easier than before, by using a blockchain such as the Bitcoin blockchain.

Recent news, which we find very interesting, is that *BBC news* [34], on May 2016, published that Craig Wright, an Australian entrepreneur, claimed that he is Satoshi Nakamoto, i.e., the inventor of Bitcoin. The Bitcoin community confirmed his claim, and he further proved his claim by signing blocks by using cryptographic keys that were used in the early stage of the Bitcoin invention.

6.2. Future work

An analysis framework for the characteristics of the blockchain is needed, as it would be a useful tool in similar future studies.

A suggestion for the future work is to continue this work by conducting more interviews in order to identify some additional characteristics for the current application areas of blockchain. In particular, the transparency aspects are important to study in more detail.

Another suggestion is to find out a way to analyze the blockchain technology focusing on security aspects. This could be made possible by conducting some field studies in different companies that are using the blockchain in their solutions, and to study their problems (if they have any) with the blockchain in order to prevent future problems with the blockchain.

In addition we are interested in analyzing the smart contracts in more detail and study the potential risks within this area. An interesting idea is to find out if there are any privacy problems in the smart contracts. In addition to these findings, we can identify possible solutions to solve the above problem, if there are any.

Another interesting aspect of blockchain is to study the challenges of the usage of this technology in banking. There are truly some challenges in this area, which need to be studied.

References

1. Nakamoto S., Bitcoin: A Peer-to-Peer Electronic Cash System, http://www.bitcoin.org, 2008, 2016-01-06

2. Bradberry D., Inblocks, Engineering and Tecknology magazine, www.EandTmagazine.com, 2015

3. Creswell J. W., Research design: Qualitative, Quantitative, and Mixed Methods Approaches, Third Edition, SAGE Publications, 2009

4. Bitcoin, https://bitcoin.org/en/how-it-works, 2016-01-07

5. Namecoin, https://wiki.namecoin.org/index.php?title=FAQ#What_is_the_relationship_of_this_project_to_Bitcoin.3F, 2016-01-10

6. Fromknecht C., Velicanu D., Yakoubov S., A Decentralized Public Key Infrastructure with Identity Retention, 2014

7. Tewari H., Noallain E. O., Netcoin: A Traceable P2P Electronic Cash System, IEEE International Conference on Web Services, 2015

8. Lazarovich A., Invisible Ink: Blockchain for Data Privacy, 2015

9. Kosba A., Miller A., Shi E., Wen Z., Papamanthou C., Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, 2015

10. Zyskind G., Nathan O., Pentland A. S., Decentralizing Privacy: Using Blockchain to Protect Personal Data, IEEE CS Security and Privacy Workshops, 2015

11. Onecoin, http://onecoinmalmo.nu/onecoin/fem-skal-till-att-blockchain-kommer-att-revolutionera-varlden/, 2016-04-06

12. Higginbotham S., Check out IBMs proposal for an Internet of things architecture using Bitcoina´s block chain tech Gigaom. https://gigaom.com/2014/09/09/check-out-ibms-proposal-for-an-internet-of-things-architecture-using-bitcoins-block-chain-tech/ 2014.

13. Onename. Decentralized identity system built on the blockchain. https://onename.com/, 2013

14. ChangeTip. A Love Button for the Internet. https://www.changetip.com/, 2013.

15. Coin market cap, https://coinmarketcap.com/all/views/all/, 2016-04-06

16. Mougayar W., Oreilly. https://www.oreilly.com/ideas/understanding-the-blockchain, 2016-03-22

17. Goldberg D., DiGITAL, http://digital.di.se/artikel/storbankerna-sluter-upp-bakom-blockkedjan, 2016-03-17

18. Kelly J., REUTERS, http://www.reuters.com/article/global-banks-blockchain-idUSL8N12S2OG20151028, 2016-04-04

19. Kiat O. K., E27, https://e27.co/now-herald-age-blockchain-smart-contracts-20160120/, 2016-04-02

20. Kelly J., REUTERS, http://uk.reuters.com/article/uk-banking-trading-blockchain-idUKKCN0UY28W, 2016-02-20

21. Kharpal A., CNBC, http://www.cnbc.com/2015/12/31/blockchain-what-the-big-banks-say-about-the-tech.html, 2016-03-24

22. Swan M., Blockchain Thinking: The Brain as a DAC (Decentralized Autonomous Organization. Texas Bitcoin Conference, 2015

23. Swan M., Blockchain: Blueprint for a New Economy. Sebastopol, CA: O'Reilly Media, 2015

24. Juels A., Kosba A., and Shi E., The ring of gyges: Using smart contracts for crime. Manuscript, 2015

25. BreakIT, http://www.breakit.se/artikel/2403/12-branscher-som-blockchain-tekniken-kan-forandra-i-grunden, 2016-04-01

26. Dwyer G. P., The economics of Bitcoin and similar private digital currencies, Journal of Financial Stability,vol 17, 81–91, 2015

27. Oates B. J., Researching Information Systems and Computing. SAGE Publications Ltd, 2006

28. Casey M. J., THE WALL STREET JOURNAL, http://blogs.wsj.com/moneybeat/2014/12/02/bitbeat-blockchain-based-id-app-reimagines-internet-identity/, 2016-04-05

29. Vigna P., THE WALL STREET JOURNAL, http://blogs.wsj.com/moneybeat/2015/09/15/bitbeat-wall-street-city-banks-join-blockchain-focused-consortium/, 2016-04-05

30. J. Cassano, Fast Company, http://www.fastcompany.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app, 2016-04-15

31. Williams-Grut O., Finance, http://uk.businessinsider.com/blockchain-r3-membership-hits-42-as-it-looks-to-non-banks-2015-12, 2016-04-18

32. Wood G., Ethereum: A secure decentralized transaction ledger. http://gavwood.com/paper.pdf, 2016

33. Mougayar W., Startupmanagement, http://startupmanagement.org/2014/12/30/blockchain-apps-moving-from-the-jungle-to-the-zoo, 2016-04-22

34. BBC, http://www.bbc.com/news/technology-36168863, 2016-05-11

35. Bit4m, http://www.bit4m.org, 2016-05-13

36. Norta A., Ma1 L., Duan Y., Rull A., Kõlvart M., Taveter K., Journal of Internet Services and Applications, vol 6:8, 2015

37. Liebenau J., Elaluf-Calderwood S. M., Blockchain Innovation Beyond Bitcoin and Banking, March 18, 2016 Available at SSRN: http://ssrn.com/abstract=2749890

38. La'Zooz, http://www.lazooz.net/whitepaper.html, 2016-05-12

39. MaidSafe, http://maidsafe.net/safecoin.html, 2016-05-12

40. Bitnation, https://bitnation.co/notary/ 2016-05-13

41. OpenGarden, https://opengarden.com/ 2016-05-13

42, Hinkes A., Coindesk, The Law of The DAO, http://www.coindesk.com/the-law-of-the-dao/, 2016-05-20

43. Gibson W., Device democracy, Saving the future of the Internet of Things, 2015, Accessed on: http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF, 2016-05-23

44. Buterin V., A next generation smart contract and decentralized application platform, Etherum White Paper, April 2016, Accessed on http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, 2016-05-10

45. BBC, http://www.bbc.com/news/business-35370304, 2016-05-23

46. Swish, https://www.getswish.se/om-swish/, 2016-05-27

Appendix A

Interview guide, first interview

The questions are divided in two categories: general and specific questions

Inform about:

- I believe that this interview will take an hour
- Anonymity
- A summery will be send to the interviewee(s)
- Is that ok to record the interview?
- Interviewee don't have to answer all the questions and can stop when he/she wants to
- The aim of the interview is to help us identify characteristics of blockchain and understand blockchain
- We need to plan a second interview for evaluation of the results we have got

General questions:

1. Please describe your blockchain technology
2. What are the main characteristics of the blockchain?
3. What are the strengths of the blockchain?
4. What are the weaknesses of the blockchain?
5. What do you believe about the progress of blockchain in the future?
6. Do you believe that blockchain might be the answer for managing private and sensitive data on the Internet?
7. Do you know about any other application areas of the blockchain?
8. Do you know about any other companies who work with the blockchain?

Specific questions:

9. Why did you choose Blockchain for your system/solution?
10. Did you consider any other solution to use in your system instead of blockchain?
11. Why did you choose blockchain instead of any other solution?

Appendix B

Interview guide, second interview

The questions are divided to the two categories: general and specific questions.

Inform about:

- I believe that this interview will take half an hour
- Anonymity
- A summery will be send to the interviewee
- Is it ok to record the interview?
- Interviewee don't have to answer all the questions and can stop when he/she wants to
- The aim of the second interview is evaluation of the results we have obtained, and to identify if the obtained results are consistent with the view of the interviewee.

RQ1: what are the current application areas of blockchain?

1. Which application areas do you know that currently use blockchain?
2. What do you know about these application areas?

If one or more of the following application area are not mentioned:

3. Do you agree with these application areas as well?
    - Money transaction
    - Decentralized privacy and data protection
    - Smart contract
    - Secure identity
4. Do you know any companies working within the application areas that you mentioned?

RQ2: what are the possible application areas of blockchain?

5. Which application areas do you suggest that can possibly use blockchain?
6. What do you know about these application areas?

If one or some of the following application area are not mentioned:

7. Do you agree with these application areas as well?
    - Supply chain management
    - Mind files, storing memories to use in the future when sick
    - Secure identity that can help to access any personal information
8. Do you know any companies working within the application areas that you mentioned?