Universitetet
i Stavanger

FACULTY OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS

Study programme/specialisation: Risk Management	Spring semester, 2018 Open
Author: Jason Duy Thong Do	…………………………………………… (signature of author)

Programme coordinator:

Terje Aven

Title of master's thesis:

Blockchain: Risk Analysis Issues, Potential and Opportunities

Credits: 30

Keywords: Blockchain, Risk, Risk Analysis, Risk Management, Risk Assessment, Supply Chain, Risk Management	Number of pages: 44 + supplemental material/other: 0 Stavanger,15th June 2018 date/year

Blockchain Technology: Risk Analysis Issues, Potential and Opportunities

Master's Thesis

by

Jason Duy Thong Do

Stavanger, 15th June 2018

Universitetet
i Stavanger

Acknowledgements

First of all, I want to show my gratitude to my supervisor Terje Aven for providing me the opportunity, and for guiding me through the process with his knowledge and expertise. This wouldn’t have been possible without him leading me on the right path. Secondly, I want to thank friends and family for assisting and supporting me through the whole process.

Abstract

The purpose of this thesis is to first give a fundamental understanding of blockchain technology. And secondly, to look at opportunities blockchain technology has within various industries. Additionally, I am seeking to understand the risk introduced in blockchain implementation and the challenges posed in a risk analysis. Blockchain technologies are decentralized distributed ledgers that underlie the technology and infrastructure for Bitcoin and other cryptocurrencies. The main aspects of blockchain technology is its decentralized, transparent, immutable, encrypted, and robust nature. Risk analysis' main purpose is to describe, present, and understand risk in a systematic and informative way, to support a decision-maker. Where risk analysis issues are determined by assessing the strength of knowledge and the understating of associated uncertainties. A model for *inhibitors of disruptive innovation capabilities* is used to evaluate the challenges of implementing blockchain. This is done to identity challenges (new risk and high uncertainty) that implementation of blockchain brings to whatever filed or industry it is introduced into. There are many issues within the technology that must be further explored and troubleshooted before the commercialization of blockchain is viable. Because of this, further developing of the technology and growing of a strong knowledge base will result in a reduction of associated risk. This untimely enabling blockchain technology to be feasibly introduced into multiple fields.

Table of content

1. Introduction

After Satoshi Nakamoto's publication of a white paper describing the idea of Bitcoin and the rapid growth of cryptocurrency, blockchain technology has been recognized for its potential. Bitcoin has repeatedly made headline after headline; however, the underlying technology is blockchain. This makes it difficult to connect and distinguish both from each other and often mistakenly use interchangeable language. Having a clear understanding of blockchain is important when trying to comprehend the possible uses. In this burgeoning filed, research has discovered that blockchain's application has a wider breath beyond cryptocurrency. Any industry or field that could utilize blockchain's attributes: decentralization, transparency, immutability, traceability, and trustless transactions, will benefit from implementing it. One such industry is that of supply management as well as the banking industry. Blockchain has the potential to revolutionize, fundamentally, how many fields and industries operate. Possibly replacing legacy systems and resulting in more efficient systems. Additionally, *smart contracts*, with the characteristic of enforceable code, can restrict and set conditions for execution. This tool can change how risk is managed; in a systematic and controlled way. Even so, because blockchain is still quite new and not developed enough to be commercially viable, the introduction of new risks must be considered and addressed.

1.1 Thesis's objective

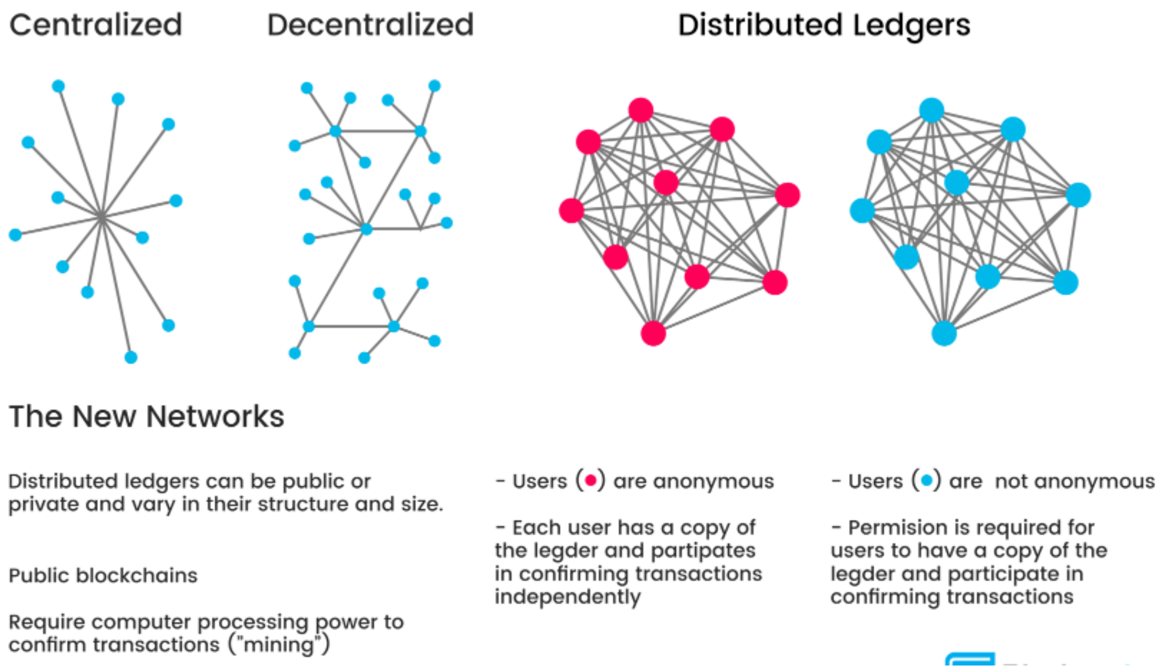
The main objectives of this thesis are first to provide a basic understanding of how blockchain technology operates and secondly, to give insights into applications areas that go beyond cryptocurrency. The other objective is to address the issues of conducting a risk analysis for blockchain and eventually discuss the reasons why blockchain is a strong tool for the field of risk management.

2. Blockchain Technology

Blockchain is the underlying technology and infrastructure for Bitcoin and other cryptocurrencies. Originally developed to function as a database, it is an effective way to record transactions in a decentralized manner. Making it independent of any central authority. This peer-to-peer system, where no intermediary is needed to establish trust, is a trustless system where parties do not need to trust each other to do transactions. Thus, eliminating issues of fees and time within the transaction process.

2.1 What is blockchain technology?

The main aspects of blockchain are its decentralized, transparent, immutable, encrypted, and robust nature. It is a distributed ledger that can either be public or private, operating with permission or permissionless. But what does it mean to be a distributed ledger? It can be thought of as a distributed database that consists of a network of nodes each having a copy of the ledger which are continuously updated. Breaking it down into a simple concept, one can look at google docs for the representation of this model. Everyone who has permission to access specific documents in google docs has (1) access and (2) is continuously updated. However, the files on google docs are centralized information. They are accessed through Google’s servers and edits happen in the document. In contrast, in the blockchain distributed ledger, information can only be added to the ledger and not deleted or altered.



The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous

- Each user has a copy of the legder and partipates in confirming transactions independently

- Users (●) are not anonymous

- Permision is required for users to have a copy of the legder and participate in confirming transactions

Figure 2.1 Distributed ledgers (Rosic, 2016)

Blockchain's main use is for conducting transactions of value, such as cryptocurrency, records, contracts, assets or other kind of information. When a party requests a transaction within the blockchain distributed ledger, the request is announced to all the other nodes in the network. These nodes, computers in the network that have a copy of the ledger, validate the transaction and the user's status. This is conducted through the use of known algorithms. For example, bitcoin uses proof of work as the validation method with three characteristics: (1) computationally difficult (2) costly to produce (3) and easy to verify. Once the initial party's transaction is verified, it is combined with other transactions and a *block* is created in the ledger. The *block* is then added to the existing blockchain in a way that is permanent and immutable. This permanence is accomplished by making the new *block* connect to the previous *block* hence the name blockchain. A corruption in a block will make the whole chain invalid. Even so, since the ledger is not centralized like other networks, a corruption will not pose as a problem. It is important to note that in theory it is possible to take over a blockchain system. However, in practice it is highly unlikely due to it requiring an enormous amount of computational power just to take over 51% of the nodes.

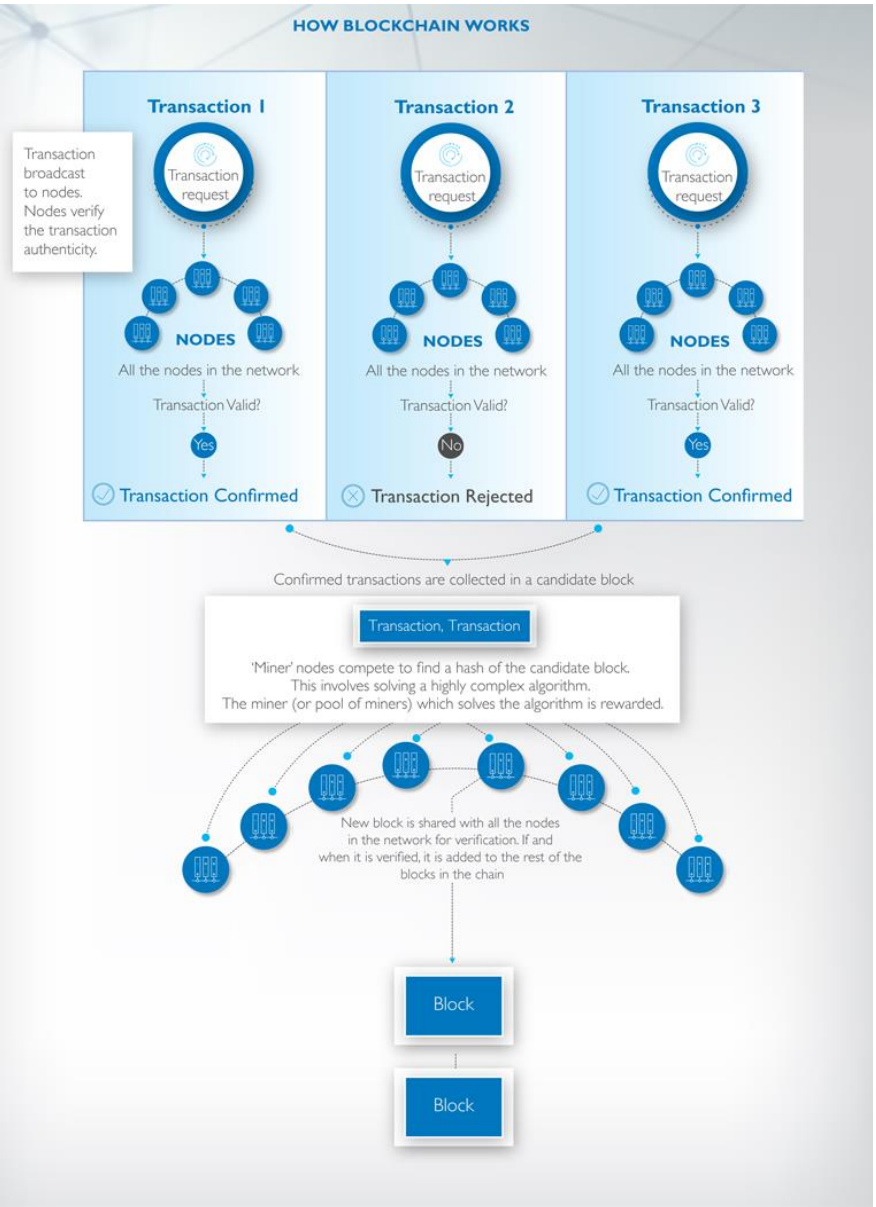

HOW BLOCKCHAIN WORKS
Transaction 1
Transaction 2
Transaction 3
Transaction broadcast to nodes. Nodes verify the transaction authenticity.
Transaction request
Transaction request
Transaction request
NODES
All the nodes in the network
Transaction Valid?
Yes
Transaction Confirmed
NODES
All the nodes in the network
Transaction Valid?
No
Transaction Rejected
NODES
All the nodes in the network
Transaction Valid?
Yes
Transaction Confirmed
Confirmed transactions are collected in a candidate block
Transaction, Transaction
'Miner' nodes compete to find a hash of the candidate block. This involves solving a highly complex algorithm. The miner (or pool of miners) which solves the algorithm is rewarded.
New block is shared with all the nodes in the network for verification. If and when it is verified, it is added to the rest of the blocks in the chain
Block
Block

Figure 2.2. How blockchain works (McKinlay, 2018)

2.2 Blockchain applications and implementations

2.2.1 Smart contract

Blockchain was initially developed to facilitate transactions of cryptocurrency such as Bitcoin. Through further development by entrepreneurs, technology is now used to code *smart contracts* that can be uploaded to the blockchain. *Smart contracts* have the parts and terms that makes up a traditional contract with an improved benefit of executing when pre-programmed specified conditions are met. These types of contracts are decentralized and do not require a third-party service as intermediary to enforce or to keep record of. And so, eliminating “ambiguity regarding the terms of the agreement and disagreement concerning the existence of external dependencies.” (kakavand, 2017)

Since contracts are enforced by computational coding, the need for trust between parties is removed from the equation. This “trustless” system, where transactions between parties are monitored, validated, verified, and enforced by the blockchain, provides improved security and a reduction in transaction time and cost associated with contracts.

2.2.2 Banking and payments

Traditionally in the banking industry the clearing and settlement of financial assets is a lengthy process with higher opportunity of risk. The process of “clearing consists of several steps: matching the trade compares the records of both buyer and seller as to price, quantity, and other terms. Thereafter, the parties identify the accounts to which a security or payment is to be credited. Risk of failed trades is further minimized by interposing a central counterparty (CCP) between the dealers for either party. The CCP acts as seller to all buyers and vice versa, minimizing failure risk through set-off buy and sell transactions” (Caytas,2016). While the process of “settlement involves the exchange of consideration: security against payment. In advanced financial markets, physical certificates are seldom held (as a matter of authentication). Rather, they are held indirectly through a book entry system run by a custodian, typically a central securities depository (CSD), which transfers ownership on its records upon evidence of payment.” (Caytas,2016). Looking at the processes within themselves there are a multitude of steps that are contingent on others creating dependencies and delays. But it is in the relationship between each process where risk increases and an opportunity for streamlining exists. The delay from the point in which the trade is made until the time it settles creates credit and liquidity related risks. In the mitigation of these risks, blockchain technology is useful. It “can disrupt the clearing and settlement process by bringing with it decentralization and disintermediation” (kakavand, 2017). Blockchain technology makes the clearing and settlement period more efficient where they can be executed in a structured model. The entirety of the history and records of payments made for goods and assets are stored in the blockchain making trades across borders much faster, more accessible, and safe.

2.2.3 Supply chain management

“Blockchain advocates claim transparency, speed, accessibility and non-falsifiability as the cornerstones of this new paradigm.” (Apte, 2016). And this technology makes the verification of items and goods easy and legitimate. Due to the characteristics of it, it is difficult, if not impossible, to counterfeit or make illegitimates claims on the product. This allows “end users to verify exactly how, where and by whom the product they intend to purchase has been assembled and made, thereby denying a market for illegal and counterfeit products” (Apte, 2016).

However, even if the transactional records in the blockchain can be transparent and immutable, the physical product is a separate case. These records can have no indication that the product is unaltered in transit within each step of the supply chain. So, the record in the blockchain can be no guarantee to the actual whereabout of the physical product or that it has not been tampered. But what the blockchain implies in its immutability is that the transaction record and data inputted within it are not tampered with and are accurate records of history.

When the posing challenges are addressed by blockchain technology, it will reduce risk, delays, and human error. This is due to its properties as transparent, permanent records and secure monitoring. Beyond record keeping, in terms of efficiency, “it can also be used to monitor costs, labor, and even waste and emissions at every point of the supply chain” (Futurethinkers, 2017). Additionally, because consumers and companies are increasingly concerned with ethical standards in products they consider purchasing, the “distributed ledgers provide an easy way to certify that the backstories of the things we buy are genuine” (Rosic, 2016). And the additional data and track record helps to understand the economic and environmental impact the product has.

2.2.4 Government operations and Voting

Governmental operations and system are often outdated, slow, opaque and prone to corruption. Many records have not been digitized, and only exist in physical form as an old archive. This can be due to lack of resources or knowledge. Even so, the system is inefficient with a large margin for error. By implementing blockchain based systems, governmental operations can significantly improve security, efficiency, and most importantly create transparency of their operations. Transparency and public accessibility will increase trust and reduce corruption. A country already utilizing this concept is Dubai. They aim to transfer all their government documents to a blockchain system by 2020. (Ereiqat ,2017) For a government to function for its people, trust in the system is a measure which needs to always be considered. We can easily see how in developing countries transparency is key when it comes to voting. However, even in established countries like United States, where election tampering in their current voting system is suspected, an updated technology like blockchain is beneficial (Koven, 2016). With a blockchain based system voting could change to be verifiable, auditable, transparent and secure. Additionally, *smart contracts* enable automatization in the process which makes it less prone to human error or tampering. And the framework of a blockchain system does not allow for attacks from outside parties to interfere with the data.

3. Risk Analysis in Blockchain

Blockchain technology is a versatile technology that comes in all sizes, shapes, and utilizations. Because of this, just approaching risk analysis in blockchain technology from a general perspective would be difficult. In a general analysis, issues identified are similar to what an applied system like, supply chain, would encounter. And there exists much of the same issues when doing a risk analysis on blockchain related systems. The implementations mentioned in section 2.2 are all in the planning and developing stages and, as of yet, have not become commercialized or widely used. The only exception to this is cryptocurrencies. This form is in operation in real time and has been popularized by currencies such as Bitcoin and Ethereum. So why have other forms not been adopted yet? The issue is that there is lack of knowledge about how the blockchain systems can, as well as an obliviousness to, exist beyond cryptocurrencies. And this is common throughout all forms of blockchain technology since they are fairly new and are continuously changing at a rapid speed. In whatever field or way in which the technology is implemented, it will most likely be one of the first, if not the first, implementation and use of blockchain technology.

3.1 Purpose of Risk analysis

Risk analysis' main purpose is to describe, present and understand risk in a systematic and informative method. In this way a *risk picture* is formed which illustrates different factors that lead up to an initial event such as a blockchain hack that take over a whole system. The *risk picture* does not just illustrate all the factors that may lead up to the event, it also describes all the possible consequences. Identifying the initial events are important tasks in a risk analysis. It allows for the events to be analyzed, measured, understood and treated. In the *risk picture*, preventive measures are also introduced. Measures such as education on personal security or having hardware security modules installed ("hardware security modules, HSM, are dedicated hardware systems specifically designed to store and manage private and public keys" (Boireau, 2018)). The consequence reducing measures prevent the outcome from becoming a severe undesirable consequence. For example, conducing a system reset and or installing security updates. There are a lot of factors that affect the occurrence of the initial events, such as risk-influencing or performance- influencing factors (Aven, 2015). Examples of this are, the current state of the blockchain systems, the effectiveness of HMS, system reset and security updates. Then there is what is known about the hack and what could have caused it; outdated security, human error, hardware flaws and public networks. Initiating events are not only negative undesirable events but can also be events which will result in opportunity. Identifying relevant initial events and creating a *risk picture* is what risk analysis obtains; with the main intent to describe the risk. The three main categories of risk analysis methods are Simplified risk analysis, Standard risk analysis, and Model-based risk analysis which are described in the appendix (Aven, 2015).

3.2 Importance of Risk Analysis

Risk analysis can be conducted at any stages or phases in a system, no matter if it is in the early conceptual phases or the end stage of a system. The importance of the risk analysis will still remain. Whether it is to meet requirements or utilize the assets to its full potential. In the end, the risk analysis is a tool to support a decision-maker with information that will balance different concerns the decision-maker finds important. By obtaining a *risk description* it is possible to compare different solutions and measures in terms of the risk and identifying important factors in the system. Analyzing and assessing the various alternatives show different effects measures have on risk. Which in in turn gives the decision-maker an easier time to decide on what measures are the most desired and effective in the considered situation.
The design of a system is broken down into two phases, planning and operational. In the planning phase there is considerably more flexibility compared to the operational phase. Solutions are countless but detailed information is limited. Doing a risk analysis renders more information and knowledge in regard to the different solutions. Hence it will be a coarse risk analysis until more knowledge is obtained and a more detailed analysis can be conducted. Because decision-maker operate with deadlines

in mind, a long extensive analysis is not desirable. Additionally, since the analysis' purpose is to affect the decision, a balance of precision and time constraint are important.

In the operational phase there is more information available to conduct an analysis. This information can be things such as historical data. Now a detailed analysis is possible, however, the amount of measures is limited. This is due to the fact that making changes in an already operational system are more challenging than making changes in a system in the planning phase.

Blockchain can be considered both a measure for the operational phase and the planning phase. This is dependent on the perspective it is approached from. If we look at blockchain as a system to be implemented into an already operational system, blockchain will be viewed as a measure to improve performance areas and reliabilities. However, when it is looked at in the planning phase, where a system is not established and the information about the system is scarce, the development will be difficult. This will lead to a requirement for more research in order to make a successful and useful system. Since blockchains are a highly complex systems, making the right design choices for the right application will be difficult until more information and research is available.

3.3 Risk analysis process

Aven (2015) describes the risk analysis process as a central part of risk assessment and has a basic methodology regardless of the application area. The process can be done in several ways but the key features in the structures will remain. The three key elements described are:

- Planning
- Risk assessment
- Risk treatment

The basic understanding of each section could be seen in the figure 3.1, and further interest in the topic can be read at Aven (2015) p. 28-53 which describes each section more in depth.

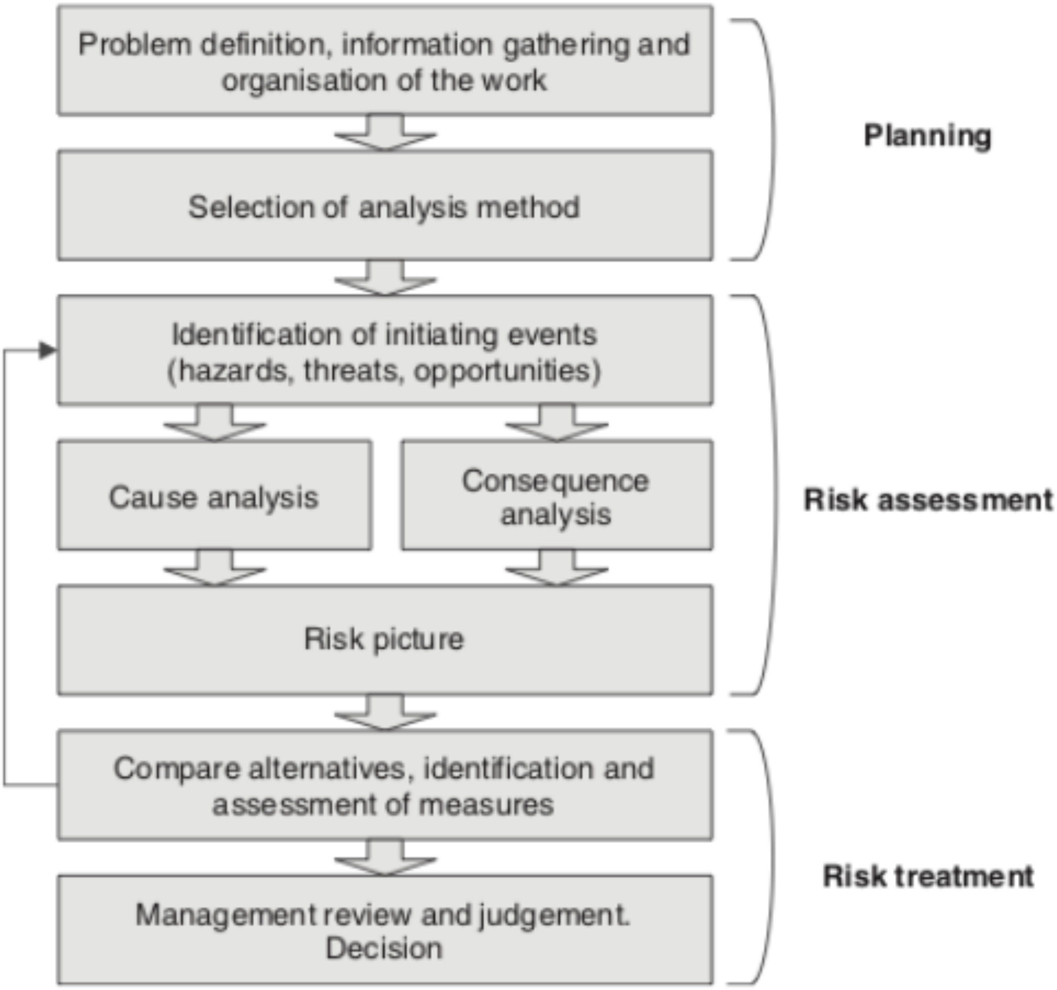

Problem definition, information gathering and organisation of the work
Selection of analysis method
Planning
Identification of initiating events (hazards, threats, opportunities)
Cause analysis
Consequence analysis
Risk picture
Risk assessment
Compare alternatives, identification and assessment of measures
Management review and judgement. Decision
Risk treatment

Figure 3.1 Risk analysis process (Aven, 2015)

3.4 The issue in blockchain

Risk analysis can be done in any stages and in any phases of a system and still be a great asset. However, obtaining information on current capabilities is reliant on current and available knowledge. Tied to this knowledge acquisition is the assessing of different possibilities when exploring solutions and actions. Because of the versatility of when a risk analysis can be conducted i.e. in what phase or stage, one cannot ignore the effects this variability has on precision and accuracy of analysis. This can be the greatest issue when doing an analysis on the blockchain related systems. Data and information regarding blockchain systems are scarce. To obtain more reliable data additional research and development needs to be invested in. And because of the clear potential blockchain has on the market, there are many companies investing in blockchain related research and development.

3.4.1 Knowledge

Flage and Aven (2009) categorize the strength of knowledge into three components; strong, medium and weak:
The knowledge is weak if one or more of these conditions are true:

- The assumptions made represent strong simplifications.
- Data/information are non-existent or highly unreliable/irrelevant.
- There is strong disagreement among experts.
- The phenomena involved are poorly understood, models are non-existent or known/believed to give poor predictions.

If, on the other hand, all of the following conditions are met, the knowledge is considered strong:

- The assumptions made are seen as very reasonable.
- Large amount of reliable and relevant data/information available.
- There is a broad agreement among experts.
- The phenomena involved are well understood; the models used are known.

Cases in between are classified as having medium strength of knowledge (Aven, 2015).

Knowledge is a crucial part of risk management. Aven (2014) states that in the traditional perspective, knowledge is made up of justified true beliefs. In a risk analysis strong knowledge regarding how a system works will result in strong arguments for reasons why a system will, for example, fail in the next year. These arguments are justified beliefs backed by experience, data, and subjective interpretation. Even so, strong knowledge will not state for certain whether a system will fail or not. An analysis will result in a better understanding and more accurate predictions then arguments based on weak knowledge. Knowledge can be expressed in many ways, a measure used often is probability; subjective probability or frequentist probability. Since much of the probabilities assigned are subjective, if different individuals do the same risk analysis the results are bound to differ.

By using the suggested strength of knowledge categories, a reasonable assumption is that the knowledge in blockchain is weak. The phenomena are poorly understood, and the model has proven to give poor predictions. A good example would be to look at Bitcoin prices which have been unpredictably volatile (Adkisson, 2018). All the main data and information about blockchain is about cryptocurrency which just shows one aspect of blockchain. The information is also in a lifespan less than a decade, which also weakens the understanding. This leads to experts having different opinions about the aspects of blockchain.

3.4.2 The Vulnerability

Vulnerability is a concept closely related to risk and is risk conditional to an occurrence of a certain event. Let us take the Bitcoin system as an example. If an event, for instance, a hack on the system occurs, what will be the associated consequences? The possibilities are dependent on the vulnerability of the system. Is the system resilient to hacks or not? Do the nodes have the latest security updates? Has the system been recently exploited and their weak points exposed? Given that an undesirable event (initiating event) has occurred, the vulnerability concept is used when there is a concern about the consequences. "Looking into the future, the consequences are not known, and vulnerability is then to be understood as the combination of consequences and the associated uncertainty"(Aven, 2015). If we say that the Bitcoin system is vulnerable, it means that vulnerability of the system is considered high. If the security of each node is outdated, it could be considered vulnerable. Hence a hack would result in a high probability of system takeover. In a system like Bitcoin, the highest vulnerability would be in the users of the system since the average user does not have the proper information security knowledge. So, events such as obtaining private keys would be possible for the experienced hacker.

3.4.3 Uncertainty Aspect

Another concept that is closely related to risk is uncertainty. Uncertainty is one of two main dimensions of risk, whereas the other is consequences. The most common tool to measure uncertainty is probability, but other measures are also used. This concept is also closely connected to knowledge. Where knowledge helps in expressing the uncertainty through methods like probability.

In blockchain there is a lot of uncertainty related issues. Uncertainty about the trajectory of where blockchain is headed. Uncertainty regarding the consequences of implementing blockchain. And uncertainty about what areas and fields blockchain will influence. As the progression of the technology gains ground, more opportunities will surface. The instances of cases which use blockchain bloomed much bigger than first intended, and it will be reasonable to assume in the future more uses cases will be thought of. Pushing boundaries into places where blockchain was never considered to be useful in.

If we think of the situation where the implementation of blockchain is in a field or industry that fits the *never considered category*, uncertainty here means not knowing what the consequences will be. That is a huge aspect of blockchain, not knowing how it can affect the field, it has the potential to improve the area, but we do not know what kind of negative effects it will produce.

The effects of blockchain can be considered a black swan(appendix), a surprising event that was unimaginable with the current knowledge. In turn, this has a serious impact in the likelihood of changing the current systems to potentially creating new fundamentals and attributes. Without the inevitable rise and popularity of bitcoin blockchain technology, would this system have been recognized and considered as a solution to different problems?

The issue is then how to handle the uncertainties blockchain introduces. Since the framework of blockchain is a distributed ledger that requires cooperation between a lot of actors. There are a multitude of systems that must be considered and in return increase in complexity. Essentially an event could potentially cause much more harm than what it seems to in the current systems. How should the uncertainty be handled in relations to events where blockchain has been implemented? In cases like this “traditional statistical methods and tools are not suitable, as relevant supporting models cannot easily be justified and necessary data are missing.” (Aven, 2014). However, other methods and approaches are available. In situations like this, method which provide robust and adaptive analysis are of importance. Tools used are based on two strategies. The first strategy is to find solutions and decision that suit a magnitude of models since there is uncertainty in which model to use. The second strategy is adaptive risk management, a technique where risk is treated by tracking multiple actions to see what effects different actions to gain relevant data and knowledge.

3.4.4 Decision making

The main reason for conducting a risk analysis is to support decision making. It often involves making decision in situation with high risk and large uncertainties. This is a challenge since it will be difficult to predict the consequences of the decisions. There is a lot that needs to be considered before a decision is made. Firstly, it starts off with a decision problem, which is the problem of choosing between different alternatives and solutions. All these different alternatives and solutions meet requirements and goals that the decision-maker and stakeholders have set. In the beginning and early stages of the decision making, a lot of different alternatives that were defined are considered. Analysis provides a basis for sorting through the alternatives and help to choose which ones should be studied further. Then the decision-maker completes a managerial review and places judgement on the various solutions and alternatives, while considering the limitations and boundaries of the analysis. Finally, the decision-maker decides on what choice or action to take. A simple model for decision-making is shown in figure 3.

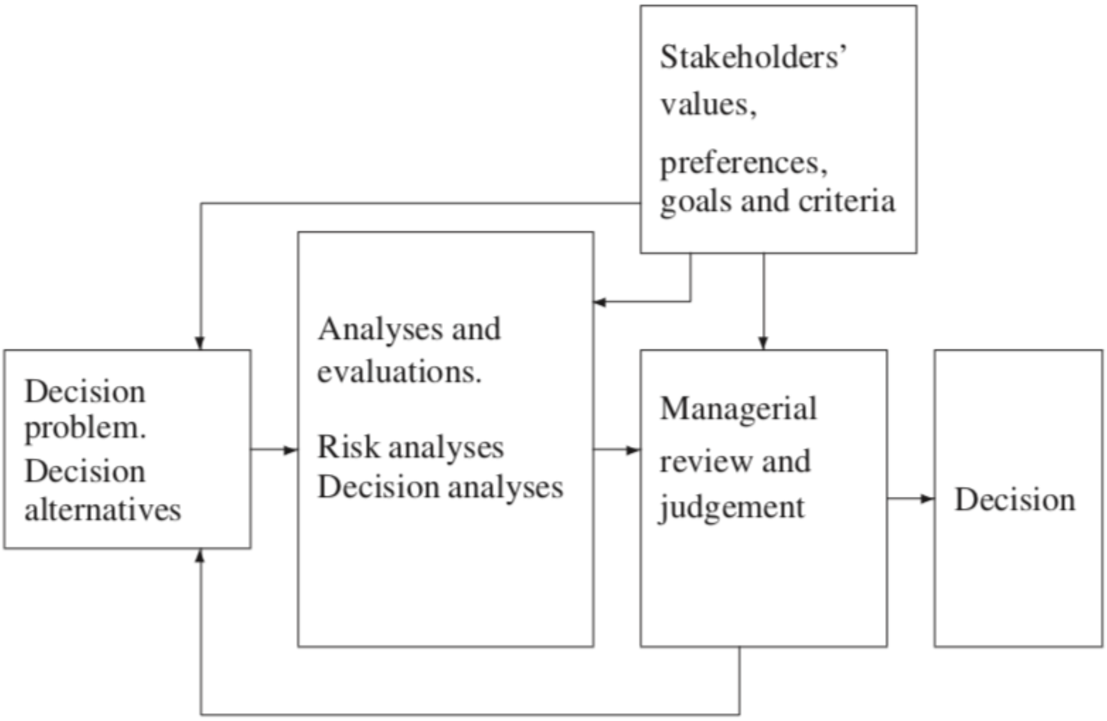


Figure 3.2 Model for decision making under uncertainty (Aven, 2015)

Decisions regarding blockchain have high risk and large uncertainties which makes deciding difficult. The decision-maker must consider the fact that the analyses produced are based on weak knowledge and simplifications. Basic support for the decision-maker seldom provide all the answers that are important for the decision-maker. There will always be some kind of limitations in the basic information. Aspects which the analyses do not consider are covered by the managerial review and judgement.

Another aspect that makes decision-making difficult in blockchain systems are communication of risk and the risk presentation. Because of the complexity of blockchain systems the decision-maker will have problems understanding the limitations and the basis information provided in the analyses. Trying to communicate in simpler manner runs the potential of losing valuable information and insight which the analyses provide. Blockchain are usually closely related to competencies across many fields which increase the complexity and the difficulty in comprehension.

4.Blockchain Technology potentials and opportunities in the risk management field

With the introduction of blockchain technology, the way risks are managed and measured, has the potential to revolutionize the risk field. This is inclusive of the possibility to conduct real time audits at any given time and the integration of programmable *smart contracts* that process transactions of assets and information. What was in the past perceived as operational risk can be partly or entirely eliminated. The loyalty and trust provided to different parties is not as necessary to a successful expansion and inclusion of more business partners around the globe. Every transaction execution can be automated and enforced through the blockchain. Furthermore, the transparency framework of the systems with its blockchain implementation and immutability, facilitates an easier option to legitimize records of any given party.

4.1 Potential in Risk management

The question is how can this affect the risk field? The answer? The potential is endless. It all depends on the development of the technology and the course of its evolution. We can already see from the first introduction of blockchain it has changed into much more than what it was first theorized to be. Staring from a distributed database and moving towards a distributed virtual machine capable of executing and enforcing code. The risk of an agreement not being met is eliminated due to this ability. To make the illustration of the concept easier to understand, we can look at a supply chain. Usually in a supply chain there are a many different suppliers that must coordinate and operate under certain quality certificates. There is a lot of risks that is involved in a supply chain. These risks include the risk of quality and quantity not matching the agreement, deadlines not being met, human error in operations, slow or bad information relay. These risks will cause problems in the supply chain. For instance, a slow information relay about a shipment that is stalled because of bad weather and will not reach the next shipping dock in time for the shipment transfer.

Finding a solution will take a longer time. Additionally, it is possible that the knowledge of a fault in operations will not be informed before the damage is already done. This is certainly a human error where the customer should be informed right away. So, if we look to blockchain for a solution, this kind of information can be relayed instantaneously when it is logged in the supply chain. Customers can check where their shipments are in real time and if there will be any deviations. There is also the possibility to put safeguards in the code which will alert the parties about deviations. This information is crucial in operations. Enabling management to agree on solutions and create an action plan. The possibilities are endless in what can be done in the code in the blockchain.

Other risks include the legitimacy of the products and agreement breaches. For example, a company not paying for services, products are made with cheaper material, or products made by a supplier without certain quality certificates affecting deadline or quantity. Essentially, every component and material recorded can be tracked to its originality, where it came from, where it has been and at what time, who made it or altered it. It is important to note that in the old system these components of blockchain can already be done, however, it is done with less efficiency and accuracy with increased variables. The process of acquiring pertinent information can take weeks or months, not including having to go through it all. While the blockchain system presents the information in an easier, accessible, transparent, chronological order, and immutable way. Making the process effortless with a decreased risk for forged documents. Agreement breaches will not pose a problem a because it will be enforced in the code. There will be conditions written in the *smart contract* that must be fulfilled to execute the process. For example, condition A, B and C must be fulfilled for outcome D to result. Thus, eliminating ambiguity in transactions and agreements. Since most of the transactions can be coded in the *smart contracts*, most of the affairs can be automated and enforced. This is a substantial tool to control the risk. Allowing for the possibility to choose which risk you want to be exposed to and totally, or partly, eliminate other risks. As mentioned earlier, risk such as human error, counterfeit products, agreement breaches, and many operational risks could be eliminated by blockchain. This versatility is applicable in far more than just supply chain. But first a blockchain system must be established.

4.2 Assink's model and the five inhibitors

Blockchain have been perceived as an ultimate solution to many problems. So why is it not already implemented and integrated into existing systems? For a new disruptive technology to be successful it is contingent on its ability to introduce new business models and solutions that are substantially better, more cost efficient and useful when compared to the previous technology. That means, that in order to commercialize the technology, it need to develop to a stage where the technology can go beyond the conceptual phase and into actual practical use. Cryptocurrencies such as Bitcoin have already proven that this technology can be used in practice. However, there is still a lot of issues that need to be addressed in order for it to be used as it was intended; a worldwide universal digital currency that does not have any attachment to a central banking or authority. Even so, the full impact of the use of blockchain is still far from achieved. There is a list of factors that inhibit a full adoption of blockchain. We will use Assink's conceptual model for *inhibitors of disruptive innovation capabilities* to assess the implementation feasibility of blockchain technology. In Assink's model, five inhibitors were identified to inhibit implementation and performance of disruptive innovations (Assink, 2006).

- Adoption barrier
- Mindset barrier
- Risk barrier
- Nascent barrier
- Infrastructural barrier

4.2.1 Adoption barrier

The main inhibitors in the *adoption barrier* is the already existing systems and organizational models which lead to reluctancy to innovate beyond the standard pattern. This attitude is seen towards the new developments of Blockchain, *smart contracts* and cryptocurrencies. They differ from the standard norm and were created to replace already established systems within the society. Bitcoin is the largest innovation among them with the sole purpose of being a fiat currency. The biggest challenge for it is the fact that many large companies' business models are central dependent. And while they might want to innovate and develop new solutions or enhancing existing ones, they must face the challenges of redesigning and reengineering their whole business models to adapt to new processes. All while keeping the daily business running with minimal disruptions. However, with the existing solutions and payments systems that are more or less already optimized for current daily usage, organizations and corporations are averse to implement. Even so, large corporation and institutions are already working on blockchain systems but are far from the stage of commercialization. Opportunities and possibilities have to evolve and be cultivated into such a stage of commercialization where the benefits of implementation outweigh the negative need to relearn and reconstruct a whole business model. Usually a cost-benefit analysis is conducted and may support the decision making. This analysis can help make an informed decision as to whether the substitution with blockchain based technology are beneficial for the organizations and customers. The last obstacle in the *adoption barrier* is the usability of the technology. At present, managing daily transactions and the cryptocurrency market is uncomplicated. Additionally, there are a variety of different exchange platforms being used by knowledgeable and less knowledgeable customers. However, like a black box, the average consumer finds it difficult to understand the underlying technology and the cryptography foundation needed to safely and securely do transactions. This in turn limits the expansion of the technology; unless it is made more consumer friendly with proper guidance. Further issues are found in things such as cryptocurrency needing to replace "traditional money." This is an issue because there are cases where it cannot mimic the full range of transactions of "traditional money." Thus, making it into an alternative for all transactions. An alternative not any simpler than traditional money. With this limited range, it poses a problem for its adoption on a larger scale.

4.2.2 Mindset barrier

The more disruptive the innovation is and the greater the technology change is, the more knowledge is required. This includes new set of skills and competencies as well as for organizations to start working in areas outside of their expertise, increasing risk or uncertain. In hand, evolving and changing is a good attribute for organizations. But the breakdown of mindset, experience, and beliefs towards the adoption of new possibilities in disruptive innovation is the challenging part. Especially when the end goal is an eventual rejection of all previous standards. And a concentration of new inexperienced territory which differ from their specialized expertise and competencies will in fact make them lose their edge in the competitive market. Nevertheless, the change of mindset needs to run parallel to the ability to address insufficiencies in capabilities and knowledge. Allowing for the movement towards the development of solutions good enough to be commercialized.

For blockchain technology the competencies are across different field which is a combination difficult to find and pioneer. As a result, sourcing for new talent is important. Given that the traditional intermediaries no longer can compete with blockchain based systems, organizations have to overcome this *mindset barrier* to stay relevant in potential new breakthroughs.

4.2.3 Risk barrier

In the introduction of new disruptive innovations new risk and high uncertainty are presented. As a result, applications and implementations in areas previously unknown or unforeseen are surfacing. With high uncertainty comes an increased risk due to the limited understanding and data about the new technology are low, or even nonexistent. Especially for organizations that must invest substantial amounts of resources (financial and human resources) in order to develop and grow the technology. In addition, organizations do not know whether the technology will have a demand for future products and services or if it will replace the preexisting systems. In most cases, the most important component is whether a return on investments is possible. There are many challenges when it comes to dealing with blockchain technology. Organizations have to go out of their expertise, find new competencies, and develop new technology and solutions that smoothly integrate with existing infrastructures, and finding successful use cases.

4.2.4 Nascent barrier

In this barrier, Assink (2006) presents the lack of creativity, foresight, and innovation process mismanagement as the crucial inhibitors against taking advantage of the disruptive innovations. The insufficiency of creativity speaks specifically to large corporations which lack motivation to nurture new creative ideas that differ from the standard norm. A component essential to the development and commercialization of innovative products and services. Foresight refers to the prediction of future needs and future markets which have not presented themselves yet. Developing products and services on the current market studies, rather than foresee the future needs, is a barrier for innovation. Mismanaging of the innovation process is a crucial aspect that needs to be avoided when working with disruptive innovations. Success requires key members to believe in the technology which in turn will negotiate and allocate resources for its development. “The single most important inhibitor for the adoption of the blockchain technology is the inability to effectively manage the innovation process” (Efpraxia, 2018).

4.2.5 Infrastructural barrier

“The infrastructural barrier aims to underline the lack of regulation, standards, processes, distributors, markets and the likes, which are required to make the disruptive innovation a fully commercialized product” (Efpraxia, 2018). When looking at blockchain based technology and its applications, it is easy to observe the presence of *infrastructural barriers*. It lacks regulation and standards. Fundamentally, the adoption of blockchain is not made on one organization’s decision. And due to the nature of the blockchain framework, it takes a whole network of corporations and businesses to collaborate on a blockchain based infrastructure. The absence of a universal standard infrastructure to smoothly support a blockchain adoption will be a barrier for early adoption and implementation. Additionally, because of the variety of networks the compatibility among the existing internal IT systems may prevent early adoption of the technology as well. “It is also probably the reason behind the current attempts of many large technology providers (such as IBM or Microsoft) and industry consortia (such as R3 in the financial services industry) to set up and provide a standard, interoperable set of infrastructure services to interested users.” (Efpraxia, 2018)

4.3 Risk mitigation

As discussed in section 3.1 blockchain has the potential to change how risk is handled through the fundamental attributes of blockchain technology. Essentially blockchain could be used as a solution or an alternative to reduce or eliminate risk. The decentralized nature of blockchain could increase the reliability of a system, since there is no single point of failure like in a centralized system. Even if one or more nodes in the system are not operational, the entire system is still in order. Thus, making the system much more resilient and robust. Risk that involves transparency, trust, transactions, auditability, human error, authenticity, security and the list go on, potentially could be reduced. Also, blockchain could be used as a warning system to alert on deviations which provide management with more pertinent information. All this is possible because of the executable codes in the *smart contracts* that have pre-programmed conditions and actions.

4.4 Risk introduction

In the implementation of blockchain new risk and high uncertainty are introduced. Some risks mostly related to the technology’s operational mechanism are show in table 1.

There are many issues within the technology that need to be further explored and troubleshooted before the commercialization of blockchain is viable.
For a more detailed description and technicality of these risks and causes see (Li, 2017)

Table 1. Risk and Causes (Li, 2017)

Risk	Cause
51% vulnerability	Consensus mechanism
Private key security	Public-key encryption scheme
Criminal Activity	Cryptocurrency application
Double spending	Transactions verification mechanism
Transaction privacy leakage	Transaction design flaw
Criminal smart contracts	Smart contract application
Vulnerabilities in smart contract	Program design flaw
Under-optimized smart contract	Program writing flaw

4.4.1 Potential Operational risk

Blockchain is a decentralized software that is comparable to centralized system software. Any software can have the same type of operational risk, but the decentralized systems might introduce more difficulties. Even so, there are no perfect software systems. This is because software is developed by humans which unavoidably introduces human errors. Understanding this, we can see how this makes blockchain vulnerable to cyberattacks and bugs. Blockchain are constantly altered through changes and updates, which again introduce new bugs and vulnerabilities. A successful attack on the system could result in tampering with the blockchain which highly damages the credibility and reliability of the system. In its present form, there has been many hacks and attacks on the cryptocurrency systems which have resulted in loss of huge financial assets. Such as the recent hack on Contrail, a Korean based crypto exchange, which lead to a loss of $40 million USD. Beyond hacks, ever-changing software is more problematic to decentralized systems than centralized systems because updates can be unevenly adopted into the networks due to disagreements among the participants in the network. This potential problem is mostly connected to public blockchains. While private blockchain requirement can be set to take part of the blockchain. Lastly, the complexity of blockchain result in a limited amount of people who fully understand how it operates. This puts tremendous pressure and trust on the people managing the blockchain network to make good decisions. As the blockchain system grows and becomes larger and more corporations start utilizing the blockchain network, the importance of these blockchain experts increase. Because the experts must implement beneficial guidelines correctly and securely into the system code, the creation of complicated systems that have crucial importance must be done with care and foresight.

The decentralized structure of blockchain introduces new operational risks. First, because the systems are not owned by any single entity, no one is responsible for keeping the systems operational. For example, public blockchains like that of Bitcoin. Consequently, when the need for critical repairs (which can result in system collapse) arises, there is no one with the sole responsibility to repair the system. The developers that have worked with the code can choose to not engage in the moment of crisis if they feel like it. Additionally, implementing a solution would still take a much longer time due to the lack of a central authority and central decision-maker. An individual can merely purpose a solution to the community, but it is up to the community to successfully implement the solution. Which is why decentralizing vital components in society would pose huge risk for its functionality and stability (Kakavand, 2017).

5. Conclusion

In this thesis, we looked at the difficulties of implementing blockchain technology and concluded it to be a new *disruptive innovative technology* with a lot of room for growth. By using risk analysis as a tool to establish a comprehensive understanding of the current capabilities, blockchain has a huge potential to reduce risk and make enormous impacts to current systems. There are some limiting inhibitors that must be addressed in the implementation of blockchain. As well as keeping in mind the considerations of new risk associated to the implementation of blockchain technology. Because of this, there is a continued need to explore and standardize the possible uses of blockchain. This will result in reduced risk all around. So, by further developing the technology and the collection of strong knowledge base, blockchain can become a helpful asset in multiple fields.

References

Adkisson J. (2018), “Why Bitcoin Is So Volatile”, Forbes, Available at https://www.forbes.com/sites/jayadkisson/2018/02/09/why-bitcoin-is-so-volatile/#509946ca39fb

Apte S. and Petrovsky N. (2016). Will blockchain technology revolutionize excipient supply chain management?, https://jefc.scholasticahq.com/article/910.pdf

Assink M.(2006), "Inhibitors of disruptive innovation capability: a conceptual model", European Journal of Innovation Management, Vol. 9 Issue: 2, pp.215-233, https://doi.org/10.1108/14601060610663587

Aven T. (2014), Risk, Surprises and Black Swans: Fundamental ideas and concepts in risk assessment and risk management, Routledge, Milton Park Abingdon Oxon.

Aven T. (2015), Risk Analysis: Second Edition, John Wiley & Sons Ltd, United Kingdom

Aven T. and Renn O. (2010), Risk Management and Governance: Concepts, Guidelines, and Applications, Springer Verlag, Berlin

Boireau O. (2018) “Securing the blockchain against hackers” https://doi.org/10.1016/S1353-4858(18)30006-0 (Accessed June 2018)

Caytas J. Developing Blockchain Real-Time Clearing and Settlement in the EU, U.S., and Globally (June 22, 2016). Columbia Journal of European Law: Preliminary Reference (June 22, 2016). Available at SSRN: https://ssrn.com/abstract=2807675

Efpraxia D. Zamani, George M. Giaglis, (2018) "With a little help from the miners: distributed ledger technology and market disintermediation", Industrial Management & Data Systems, Vol. 118 Issue: 3, pp.637-652, https://doi.org/10.1108/IMDS-05-2017-0231

Ereiqat S. Blockchain in Dubai: Smart cities from concept to reality, (April 10, 2017), https://www.ibm.com/blogs/blockchain/2017/04/blockchain-in-dubai-smart-cities-from-concept-to-reality/

Flage R., Aven T. (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis. Reliability and Risk Analysis: Theory and Application. Futurethinkers.org, 19 Industries The Blockchain Will Disrupt,(June 16, 2017) Available at URL: https://futurethinkers.org/industries-blockchain-disrupt

Giancaspro M. (2017), “Is a ‘smart contract’ really a smart idea? Insights from a legal perspective,Computer Law & Security Review, Volume 33, Issue 6, pp. 825-835, Available at https://doi.org/10.1016/j.clsr.2017.05.007

Hao Feng, Chan Choong Wah, (2002) "Private key generation from on-line handwritten signatures", Information Management & Computer Security, Vol. 10 Issue: 4, pp.159-164, https://doi.org/10.1108/09685220210436949

Investopedia.com, Fiat money. Available at https://www.investopedia.com/terms/f/fiatmoney.asp

Kaal , Wulf A. and Dell'Erba, Marco, Blockchain Innovation in Private Investment Funds - A Comparative Analysis of the United States and Europe (July 14, 2017). U of St. Thomas (Minnesota) Legal Studies Research Paper No. 17-20. Available at SSRN: https://ssrn.com/abstract=3002908

Kakavand, Hossein and Kost De Sevres, Nicolette and Chilton, Bart, The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies (January 1, 2017). Available at SSRN: https://ssrn.com/abstract=2849251

Koven J. "Block The Vote: Could Blockchain Technology Cybersecure Elections?" (August 30, 2016) https://www.forbes.com/sites/realspin/2016/08/30/block-the-vote-could-blockchain-technology-cybersecure-elections/#416a36942ab3

Li, Jiang, Chen, Luo, Wen, A survey on the security of blockchain systems (August 23, 2017). Available at URL: https://ac.els-cdn.com/S0167739X17318332/1-s2.0-S0167739X17318332-main.pdf?_tid=e9cdf98a-06ae-4a4d-a5a7-10e35fadb327&acdnat=1525802175_bb1e35ce184617d7370bc79b42863a1c

McKinlay J., Pithouse D. , McGonagle J. and Sanders J.(2018) “Blockchain:background, challenges and legal issues” https://www.dlapiper.com/en/denmark/insights/publications/2017/06/blockchain-background-challenges-legal-issues/ (accessed June 2018)

Nakamoto S.(November 2008) , “Bitcoin: A peer-to-peer Electronic cash system” , available at https://bitcoin.org/bitcoin.pdf

Robitzski D. (2018), “Recent Cryptocurrency Hacks Are Shaking Investors’ Faith” , Available at https://futurism.com/cryptocurrency-hacks-shaking-investors-faith-coinrail/

Rosic A. (2016), What is Blockchain Technology? A Step-by-step Guide for beginners, https://blockgeeks.com/guides/what-is-blockchain-technology/

Appendix

This appendix consists of some explanation on terms and concepts related to blockchain and risk.

Blockchain related

Smart contract

Fundamentally, a smart contract is a computer program which verifies and executes its terms upon the occurrence of predetermined events. Once coded and entered into the blockchain, the contract cannot be changed and operates in accordance with its programmed instructions. (Giancaspro, 2017)

Public and private blockchains (permissioned and permissionless)

A blockchain network may be public and open (permissionless) like the internet or structured within a private group like an intranet (permissioned). The blockchains that have captured the imaginations of many financial institutions are known as “private” or “permissioned” blockchains because only certain pre-approved participants may join them. These blockchains use a variety of means to ensure the identity of parties to a transaction and to achieve consensus as to the validity of transactions. The entities creating the “private” blockchain agree on rules that govern how entries are recorded and under what circumstances they can be modified. Only specific authorised participants are given access and are known within the network. (McKinlay, 2018)

Public blockchains: a public blockchain is a blockchain that anyone in the world can read, anyone in the world can send transactions to and expect to see them included if they are valid, and anyone in the world can participate in the consensus process — the process for determining what blocks get added to the chain and what the current state is. As a substitute for centralized or quasi-centralized trust, public blockchains are secured by crypto economics — the combination of economic incentives and cryptographic verification using mechanisms such as proof of work or proof of stake, following a general principle that the degree to which someone can have an influence in the consensus process is proportional to the quantity of economic resources that they can bring to bear. These blockchains are generally considered to be "fully decentralized" (Kaal, 2017)

Fiat currency

Fiat money is currency that a government has declared to be legal tender, but it is not backed by a physical commodity. The value of fiat money is derived from the relationship between supply and demand rather than the value of the material from which the money is made. (investopedia.com)

Bitcoin

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone. (Nakamoto, 2008)

Ethereum

Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference. These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middle man or counterparty risk. (Kaal, 2017)

Proof of work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof- of-work system similar to Adam Back's Hashcash, rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.

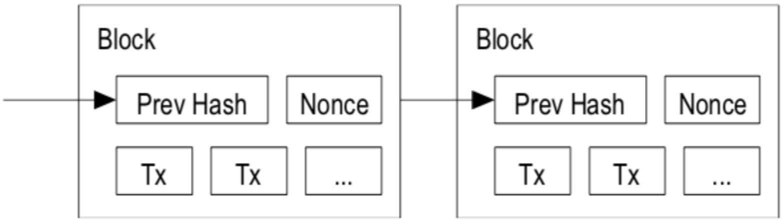


Figure A Block creation

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.(Nakamoto, 2008)

Digital signature-Private key and Public key

All digital signature technologies employ a public key infrastructure, or PKI. Under public key infrastructure, an individual has a pair of keys: a private key and a public key. A digital signature is obtained as the sender signs a document with his private key. When the recipients receive the signed document, they use the sender’s public key to authenticate the document and verify that it has not been tampered with in transit. (Feng, 2002)

Risk Related

Risk picture

The risk picture is established based on the cause analysis and the consequence analysis. The picture covers (A,C,C∗,P,U,K), where A refers to the initiating events, C the consequences, C∗ predictions of C, U the uncertainties associated with whether or not A will occur and about which values C will take, P the probabilities that express how likely various events and outcomes are, and K is the background knowledge for the predictions and probabilities. Generally, the risk picture will cover:

- predictions (often expected values) of the quantities we are interested in (for example, costs, number of fatalities);
- probability distributions, for example, related to costs and number of fatalities;
- uncertainty factors;
- manageability factors.

The point here is to reveal uncertainties and manageability factors that can give outcomes that are “surprising” in relation to the probabilities and expected values that are presented.
Depending on the objective and the type of analysis, the risk picture can be limited to some defined areas and issues. In many cases, it will be appropriate to present risk by means of a risk matrix and to discuss uncertainties and manageability factors.
(Aven, 2015)

Risk

Risk is related to future events A and their consequences (outcomes) C. Today, we do not know if these events will occur or not, and if they occur, what the consequences will be. In other words, there is uncertainty U associated with both A and C. How likely it is that an event A will occur and that specific consequences will result, can be expressed by means of probabilities P, based on our knowledge (background knowledge), K. (Aven, 2015)

Main three categories of risk analysis methods

Main categories	Type of analysis	Description
Simplified risk analysis	Qualitative	Simplified risk analysis is an informal procedure that establishes the risk picture using brainstorming sessions and group discussions. The risk might be presented on a coarse scale, e.g. low, moderate or large, making no use of formalized risk analysis methods.
Standard risk analysis	Qualitative or quantitative	Standard risk analysis is a more formalized procedure in which recognized risk analysis methods are used, such as HAZOP and coarse risk analysis, to name a few. Risk matrices are often used to present the results.
Model-based risk analysis	Primarily quantitative	Model-based risk analysis makes use of techniques such as event tree analysis and fault tree analysis to calculate risk.

Table 2. Main categories of risk analysis methods (Aven, 2015)

Black swan

Black swan as by Taleb and others are a type of surprise. In line with Aven, a black swan is seen as a surprising extreme event relative to the present knowledge/belief.

Hence the concept must always in relation to whose knowledge/beliefs we are talking about, and at what time (Aven, 2014).

Risk description

Risk is described by (C,C∗,U,P,K), where C equals the consequences of the activity (including the initiating events A), C∗ is a prediction of C, U is the uncertainty about what value C will take, and P is the probability of specific events and consequences, given the background information K. (Aven, 2015)