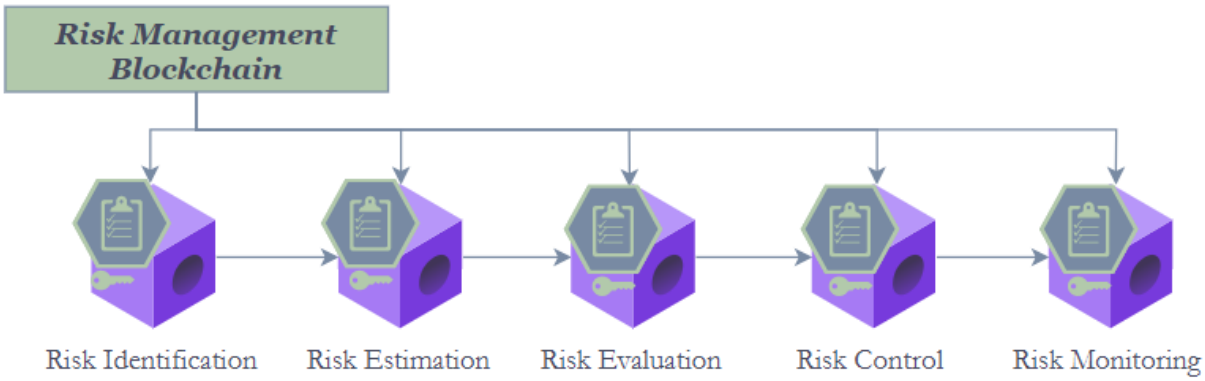
AALBORG UNIVERSITY
DENMARK

Traceability and protection of users in a risk management process with blockchain technology



Karen Patricia Flores Valverde

Jesper Nørregaard Petersen

Master Thesis

in

Master of Science in Technology in Risk and Safety Management

January 2022

AALBORG UNIVERSITY
DENMARK

Study Board of Civil Engineering
Thomas Manns Vej 23
DK 9220 Aalborg East
www.build.aau.dk

Project Title

Traceability and protection of users in a risk management process with blockchain technology

Project Type

Master Thesis

ECTS

30 points

Project Period

1/8-2021 - 7/1-2022

Education

M.sc. Risk and Safety Management

Supervisors

José Guadalupe Rangel Ramirez

Michael Havbro Faber

Group and Authors:

Karen Patricia Flores Valverde

Jesper Nørregaard Petersen

Number Printed: 91

Pages: 73

Appendix: 1

ABSTRACT

The thesis proposes a solution for how a risk management process could be adapted to blockchain technology. This proposal also considers the ability to identify the users that are working on the risk management project, by using a public key infrastructure Since blockchain is increasing attention and its use in industries other than cryptocurrencies, the thesis objective may be beneficial for future risk management communication. The system is based on a theoretical approach where the concept of architecture has been designed. A system will be proposed that combines a generic risk management process, blockchain technology and public key infrastructure. As the three systems had specific characteristics, their combination proved to have difficulties between each other, thus some modifications were necessary for the concept to be functional. The architecture showed that some of the risks are reduced when the systems are working together, but not all could be eliminated. However, the proposed architecture demonstrated that the research topic is possible. Hence, a system that could be used to identify a user's contribution to a risk management project was created, while maintaining a high level of protection and security of user information.

By signing this document, each member of the group confirms participation on equal terms in the process of writing the project. Thus, each member of the group is responsible for all contents of the project.

ABSTRACT (DANISH)

Denne specialeafhandling har udarbejdet et design, som gør det muligt at få risikostyring tilpasset blockchain teknologien. Designet giver et forslag til, hvordan man kan identificere brugere, som arbejder med et risikostyringsprojekt ved hjælp af Public Key Infrastructure. Blockchain teknologien har fået øget opmærksomhed fra andre industrier udover Cryptovalutaer, som det var designet til, hvorfor problemfeltet for denne specialeafhandling er afledt heraf. Specialeafhandlingen forklarer, hvordan denne teknologi kan give værdi for fremtidens risiko kommunikation. Specialeafhandlingen vil præsentere et system, hvor konceptet er baseret på en teoretisk fremgang og er en kombination af tre systemer. Disse systemer er Risikostyring, Blockchain, og Public Key Infrastructure. Kombinationen af disse tre systemer har vist sig at have vanskeligheder fordi, funktionerne fra de forskellige systemer ikke direkte kunne arbejde sammen. Det var derfor nødvendigt at fortage visse ændringer af systemerne, for at kunne få den for specialet fundne løsning. Designet har vist sig at kunne reducere nogle af de risici og udfordringer, der var forbundet med de enkle systemer. Det var dog ikke muligt at fjerne alle kendte risici. Det har vist sig at designet muliggør at identificere alle brugernes bidrag til risikoprocessen samtidig med, at det kan garantere høj beskyttelse og sikkerhed for brugernes personlige informationer.

ACKNOWLEDGEMENT

Jesper and Karen:

First, we would like to thank José Guadalupe Rangel Ramirez for introducing us to such an interesting topic as blockchain technology and its use connected to Risk Management. Thank you for trusting us with this topic and its development. In addition, we would like to thank you for the guidance through the thesis, without your contribution we could not have made this thesis.

Jesper:

I would like to thank my co-author, Karen Patricia Flores Valverde, for proposing me to write this thesis together. She has been critical, sceptical, with an eye for the details and helped when I had gone out off track. Her constructive inputs are a big part of the turnout for this thesis. Lastly thank you for making the thesis fun in times of frustration. And lastly, I would like to thank my family, for keeping up with me during this semester, when the thesis took a bigger part of my energy.

Karen:

I would like to thank Jesper Nørregaard Petersen for being a wonderful thesis partner who has managed to challenge me intellectually and has reminded me to constantly question everything. Thank you for your patience and understanding of my limited time because of work. Also, because every conversation and discussion has been as gratifying as educational, of which the result has been this successful thesis. Also, for bringing so much fun to the process, for believing in me and for helping me with my Danish.

I would also like to thank my boyfriend, for supporting me in this long process, for being patient, caring and understanding.

Now I would like to thank my family in our language: Gracias querida familia por creer en mi y apoyarme infinitamente sin importar la distancia. Gracias por entenderme cuando estaba ocupada y no podia llamar constantemente, por ser pacientes ya que debido a la emergencia sanitaria por covid no hemos podido unirnos durante estos años. Gracias por estar a todo momento, esucharme y guiarme. Esto es gracias a ustedes.

PREFACE

The thesis has been written as the final semester of the M.Sc. Risk and Safety Management programme at Aalborg University in Esbjerg, by Karen and Jesper, to finalize the education.

The thesis scope is to develop a concept that can answer the research topic *"How risk identification process could be framed using blockchain, which improves the traceability, proof-of-ownership, and decision making of the interested parties without compromising their protection?"* by taking existing systems and create a new variation that combines the system, and then analysed on some of the challenges that the innovative system has.

The structure for the thesis consists of eight chapters that make it easier for the readers, as presented in Figure 1. The following guidelines will apply:

Figure 1 Reader's guide

- It was written by following the American Psychological Association (APA) style for quotation and references.
- Referencing style – e.g. (Author, Year).
- Citations are written with the quotation marks "example", and with increase indent for long quotations.
- Figures and tables without references were created by the authors
- The introduction of new terms and relevant information will be highlighted in *cursive*
- Acronyms are defined by using the brackets after the term is mentioned for the first time – e.g. Example (EX).

Karen Patricia Flores Valverde

(20200028)

Jesper Nørregaard Petersen

(20200030)

EXECUTIVE SUMMARY

This thesis addresses the possibility of using ledger technology for risk management. Blockchain uses this technology with the limitation of identifying the user behind the digital address. Therefore, this thesis proposes an architecture that combines blockchain and public key infrastructure in a generic risk management. This creates a system of three components that must be analysed. The first system is the application of a risk management process useful for most cases. For the Blockchain system, the Ethereum protocol is analysed, this ledger will be considered as the risk communication of the generic process. The last system is the public key infrastructure that seeks to implement the traceability and authentication of users behind the information.

For the development of the architecture of the risk management blockchain, it was identified that not all stakeholders participate actively in the process. Those most involved in the risk management process are the risk managers, with high power and high interest. Other involved stakeholders are IT project managers and the central authorities.

The generic risk management process is sequential and consists of five stages with different steps and tasks, which are treated recursively. The development of the architecture will be based on risk identification thus in the future, it can be adapted to the rest of the stages.

Blockchain is a complex technology that considers a network adaptable for the users to access and has three layers – blockchain technology, protocol, and token. Together they make this a useful ledger for storing information immutable. For the architecture, the layers have been modified to include the credentials of the creators of the work. Also, the visualization of the blocks will be in two layers, a front page that presents work and a data page that shows the validated data to identify the author of it.

The public key infrastructure is compatible with blockchain as it provides security through the implementation of a key pair. For the implementation of a method to recognize the identity of the creators of the information, a central authority, cryptography, and a pair of keys belonging to the process were necessary. The central authority will certify the users and validate their pair of keys. The cryptography will sign all the information in the block. The process pair of keys will allow identifying the owner of the work.

The combination of the three systems was feasible by the modifications. This outlines an architecture suitable for risk management and each of its stages, steps, and tasks. Furthermore, it was possible the revocation of intermediaries when sharing information with the user that has shared write access. This technology allows adequate risk communication that will be carried out through consensus and agreements by all those involved. By adding, signed information the users will agree to the shared information, its creation and ownership.

Having a generic risk management process combined with blockchain and public key infrastructure will provide immutability, integrity, and no repudiation of the participants' work. Another advantage is that there will be constant and visible communication, with the expectation of no loss of consensus, agreements, and decisions in the process. This will help decision-makers to base their decision on complete reliable information. Despite the complex combination technologies, there are still security issues that could not be avoided. The remnants are the theft of the wallets and identities, and the hacking of the central authorities' server. Lastly, future work is programming and testing the system.

AALBORG UNIVERSITY
DENMARK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLE

ACRONYMS

ACRONYM	MEANING
CA	Central Authority
CRL	Certificate Revocation List
EC	European Commission
ECDSA	Elliptic Curve Digital Signature Algorithm
EG	Example
ERA	External risk assessor (s)
GDPR	General Data Protection Regulation
HR	Human Resources
ISO	International Standardization Organization
PBFT	Practical Byzantine Fault Tolerance
PKI	Public key infrastructure
PM	Project Manager
POS	Proof of Stake
POW	Proof of Work
RA	Registration Authority
RM	Risk Manager (s)
RMP	Risk Management Process
SHA	Secure Hash Algorithm

1 Introduction

Blockchain technology has been getting more attention over the last decade. A concept for securing the ownership of digital documents was presented by Stuart Haber and W. Scott Stornetta in 1991 (Haber & Stornetta, 1991). They saw that the evolution of audio, movies, and documents were getting more digitalised and came up with the idea of how documents could be timestamped and stored for securing documents from tampering. Nevertheless, they identified several issues with their proposed concept, such as privacy, bandwidth and storage, incompetence, and trust. As a result, they suggested that a hash function should be added to the document and a digital signature that correlates to the hash and the date-time stamp. However, due to the technology available at that time, they still had challenges.

In 2008 – under the pseudonym "Satoshi Nakamoto" – a person or a group developed the concept of Bitcoin. This digital cash system utilizes the concept of blockchain ledgers to decentralize the trust to one authority. The reason was to create a peer-to-peer network that did not use a financial institution by removing the middleman (Nakamoto, 2008). Furthermore, Nakamoto presented solutions to the challenges that Stuart and Stornetta had encountered in 1991, hence in 2009, Bitcoin went live, and so did the blockchain. Consequently, blockchain technology was now a reality rather than a concept.

Blockchain technology was first designed for a digital cash system that distributed the trust among the users without having a central authority to rely on. There has been an increased interest in cryptocurrencies, which started as one in 2008 of Bitcoin until today where there are 7.557 different cryptocurrencies (Statista, 2021). In recent years, there has been an increased focus on the technology since researchers and the industry have begun to see a practical usage for the technology in other sectors, not just finance. These sectors could be healthcare, voting, and supply chains (Kim et al., 2020).

The use of blockchain is limited primarily and associated with Bitcoin, so there is more evidence of its evolution. In addition, Bitcoin has allowed us to appreciate the kind of privacy that blockchain presents and therefore collect information about it, while in the industry, it is something relatively new. There is a misconception that bitcoin (blockchain) is untraceable, but in reality, it is simply anonymous depending on the users/owners dependences on private services, but not private at all. "*The blockchain—bitcoin's historical ledger of all transactions—is publicly viewable at all times by anyone, so that there can't be any under-the-table cash transactions"* (Galston, 2021).

The application of parameters such as the wallet address and hashes – a combination of numbers and letters – make anonymity exist, and it is not possible to identify the names or identifications of the senders and recipients. (Galston, 2021) However, all this information is recorded in each block from the beginning of the chain, which makes it traceable.

The most recent case regarding cryptocurrencies – blockchain – security is the Colonial Pipeline ransomware attack, in which 75 bitcoins ($ 5 million) were paid to regain control of the pipeline. The payment of the reward to the attackers allowed the FBI to identify a virtual currency wallet of the hackers. In this way, approximately $2.3 million was seized and recovered legally through a court order. Despite all efforts, the hackers' identity is still unknown; only the name of the terrorist group and their global location are known (Wilkie, 2021).

1.1 Relevance

While it is true that blockchain promotes the trust of the chain and its traceable transactions, the gap between the transactions and the person's anonymity remains open – the proof of ownership. For many cryptocurrencies, the anonymity and the privacy of their transactions are required and in development. However, more and more importance is given to avoiding plagiarism and corruption in terms of information. Consequently, in companies, the care of the employees and their work must be essential, which would help prevent corruption, plagiarism of information or even theft of work by a third party. In addition, as an advantage, the necessary audits and improvements will be more focused.

Blockchain is known for its key features: transparency, enhanced security, immutability, irreversible, decentralization, and faster settlements. These fundaments are applicable for a risk management process (RMP) which is defined as a *"systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk"* (ISO 73, 2009). A comparison of their characteristics is necessary to identify whether this process and this technology are compatible or likely to be combined. By comparing the characteristics, it was identified the following common characteristics:

Remove the brokers and intermediaries: Within the RMP, various and different actors could be involved, and therefore their knowledge and information must be gathered, where misunderstanding, incomplete data or omission could happen. Therefore, blockchain allows to abolish the need for intermediate partners or systems to gather the data, and simply to be managed by the owner in a block (101 Blockchains, 2020).

Need to shared write access: RMP is a shared process and involves different players; the information needs to be public and need to have shared write access for all the participants to support. This will provide integrity to the process and trust between the players since all the information will be visible at all times (101 Blockchains, 2020).

Storage of non-transaction data in large quantities: RMP has different stages; thus limited but large quantities of information must be shared and analysed at each stage. Also, each stage will rely on the previous information shared (101 Blockchains, 2020).

Rely on a trusted party: Blockchain utilizes consensus algorithms to evaluate all the transactions. The RMP could be used as a validation – of the work to be uploaded – from all the players. Furthermore, RMP must follow a regulatory factor; hence the regulators need to be included at all stages of the process (101 Blockchains, 2020; Rodriguez, 2018).

Need to have control functionality: RMP could be seen as a private process in the company, which could be implemented as a private blockchain until the process is complete. Therefore, in the RMP private blockchain, a verification code will be required to get access. There will be a need for a consensus to decide who will be involved in the process validation (101 Blockchains, 2020; Rodriguez, 2018).

Consortium Network: all transactions will be visible to the users of the blockchain. Therefore, in RMP, all information will be visible and shared with the involved actors and followed the process with the correct information (101 Blockchains, 2020; Rodriguez, 2018).

The exposed characteristics that blockchain presents and how it fits the RMP make the use of this technology suitable to create a reliable environment. However, it still has one limitation – the proof of ownership – that is why this project is relevant. Despite using blockchain technology for a process such as risk management, it is still necessary to include an additional feature to prove the owner of the work and the owner's identity. The purpose of this implementation would be to improve and create a secure environment to avoid corruption, identity theft and/or theft of the work of the employees involved in the RMP.

1.2 Audience

The audiences that this thesis is targeting are risk managers, companies developing risk-related services, and IT developers interested in applying an RMP with a strong, safe technology that provides proof of ownership of the performed work.

IT developers could be interested in creating and coding the proposed architecture to help the usage of this technology in companies looking for an RMP to be implemented.

Companies that require to implement a generic and adaptable RMP for their projects could be interested in this proposition. One should be aware of the partners' work, to recognize their work, make audits more manageable and/or prevent plagiarism and/or corruption.

1.3 Objectives

The focus of the project will be the creation of a framework that proposes an architecture of blockchain into risk management that supports the protection, identification, and traceability of ownership from individuals and companies. This will allow identifying the legitimate owner of the specific information safely. Furthermore, the proposed framework and blockchain are

intended to be applied in the early stages of risk management. More specifically, the development will consider the risk identification process.

While blockchain does not include recognition of ownership, this feature and the implicit traceability can be a vital attribute of blockchain in the application for risk management. For this reason, the research question of this project is:

How risk identification process could be framed using blockchain, which improves the traceability, proof-of-ownership, and decision making of the interested parties without compromising their protection?

To confirm this, the secondary objectives are defined as

How to validate and implement the proof of ownership to the architecture?

How will blockchain be influenced by considering an ongoing and recursive process?

1.4 Limitations

This thesis will face some limitations during the writing process and the investigation. The first limitation is related to time. This thesis was written during the winter semester of 2021, from September to December 2021. This time also limits the scope of the thesis, since not every part of the risk management process will be considered. Therefore, the architecture is only being planned for the identification of risks. This introduces our second limitation, the architecture will not consider all stages of the process, but it will be thought to be flexible and generic to be applicable in all phases; because the whole process will have the characteristic features of being sequential and recursive.

The selected topic is dominated by two areas, the first related to risk management and the second to the technological system. This thesis is subject to the domain of risk management, which means that it will focus on developing a process to manage risk using blockchain technology. Although, it will not consider all the technological factors such as block capacity, equipment needs, coding, etc. Consequently, it will not be possible to develop a technological physically and its assessment, but only a theoretical proposal.

Another technical limitation is that the Ethereum protocol was chosen to understand the technology and as a basis for the build-up of the architecture. By considering that risk management is an ongoing process, the necessary adaptations to the protocol will be developed and proposed.

Finally, another limitation that challenges this project is to find sources for this thesis. In the literature review section, it is explained that there was only found six possible documents about the topic. This situation talks about the innovative approach of the thesis at the master level. The lack of sufficient information, make this thesis purely theoretical, has no source of comparison and will not have a verification part of the work.

1.5 Definitions

Risk

The term *risk* is defined by (Joint Committee of Structural Safety (JCSS) & MH, 2008):

Risk = Consequence * probability

Risk is considered to have a negative impact on the system.

Blockchain technology

The *genesis block* is the first block of a blockchain and is the only block that can be created without a previous block to connect to (Tardi & Rasure, 2021).

A *protocol* is defined as "a set of rules that control the way data is sent between computers" (Oxford Dictionaries, 2021), which gives the guidelines that all users need to follow to exchange information.

Elliptic Curve Digital Signature Algorithm (ECDSA) is a method that is used in blockchain to generate a public key that could be connected to a private key without giving/revealing the private key. Using a function ($y^2=x^3+7$ and is called "secp256k1"), it creates 2 points based on the private key and where these two points cross the graph a third point is created that direct a straight line to a fourth point. The third and fourth points can be used to validate if the public key is connected to the private key, without identifying the private key (Antonopoulos & Wood, 2018). As presented in Figure 2.

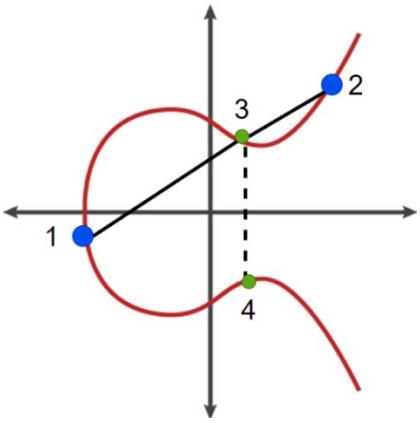


Figure 2 ECDSA, $y^2 = x^3 + 7$ (Antonopoulos & Wood, 2018)

Differences between Blockchain and Ledger technology

When talking about blockchain, often ledger technology is also mentioned. The difference between these two is that *ledger technology* is a term used for collective for all *blockchains*, while blockchain is referred to one specific ledger (Marco Polo Network, 2018).

Cryptography

Cryptography is the security of information, during communication. Cryptography consists of two parts – encryption and decryption (Martin, 2021).

Encryption is the original message that has been turned into a code; this follows specific rules on how to change the message to make it unreadable for outsiders (Martin, 2021).

Decryption allows the receiver to decode the coded message and get the original message. Both parties must agree to use the same cryptographic method (Martin, 2021).

Algorithm

An *algorithm* is a guideline used for solving problems. These are specific instructions that require specific inputs to solve a task (Downey, 2021).

2 Methodology

This document is written as the master's thesis, for the final project of the Risk and Safety Management Program. It focuses on a proposal of risk management through multiple combined systems. This section describes the intention of the eight chapters that will form the thesis, of which this is the second chapter.

Chapter 1 (introduction) will describe the history of the technology of blockchain. It will address why this thesis topic is relevant for writing and whom it is thought to gain the most use of the thesis. These will lead to the formulation of the research topic and associated sub-questions to help answer it. The chapter will also include the limitation that the thesis had and a brief description of some of the definitions that will be used and are needed to have in mind when reading the document.

Chapter 3 (literature review), an investigation will be conducted on what researchers have already done in the field that covers the topic. The investigation will be done on Web of Science to find out the results of the investigations of this specific topic. Also, it will give an idea if the topic had been covered or published, at the time of writing the thesis.

Chapter 4 (system identification) will cover the systems that are needed and who could influence the system. Since the topic required to take an innovative approach, a combination of the RMP, the blockchain, and the PKI systems, a detailed layout of the system's characteristics will be presented. First, a description of the RMP will introduce risk identification as a process. Next, the blockchain using an Ethereum protocol will be described. This will cover the different components of the technology and how it functions. Following that the PKI system will describe how it works and the keys that are needed. Lastly, two stakeholders' analyses will be required to determine the key players at the RMP, the power–interest matrix analysis and the nautic analysis: power, interest and proximity.

Chapter 5 (Architecture) will describe the concept of the thesis product. The proposed architecture will be based on the findings in chapter four. The combination of the three systems and how it functions will be covered. The modelling will take into consideration the components that need to be modified to fit the new system. The changes will be described with the respective parts of the systems and how they will interact with each other.

Chapter 6 (Analysis) an analysis of the concerns and risks that the combination of the systems present will be mentioned with the respective solutions. The reason for addressing these concerns is that the combined system will create differences compared to the original designs.

Chapter 7 (conclusion) will summarize the work and will answer the research topic describe in the introduction, based on the information acquired throughout the thesis.

Chapter 8 (Future Work) will mention the next steps that could be investigated for being able to create and develop the proposed architecture.

3 Literature review

A literature review is a tool that can be used for identifying a gap within a specific field of research by determining which terms are being used in different research fields and the associated words that are used to describe the topic. Doing a literature review is to understand what trends and patterns the field has already undergone research in. This can show the history of the field, in which directions the research is developing, and identify the gaps in the research, where little to no research has been conducted.

The database used for collecting scientific research data was Web of Science since it explores other research databases. The research field is broad for selecting the literature by only using the term *blockchain*. Afterwards, further research is narrowed down by increasing the terms used in the search and finally reading through the journals that are left. The information found in the Web of Science is imported into *VoSviewer*, which can group the research documents by co-occurrences term, called *clusterview*. The clusterview can be grouped into fields of research according to the specific terms used. The clusterview is then represented by a visual map, where it is possible to see the network and connection of the term. These connections have a link strength parameter, which indicates how strong two terms are linked together.

3.1 Broad review

In the following part, the first analysis from the Web of Science will be presented to show how the categorization is. By the time the literature review was performed, on 11 of October 2021, and by using only one term – blockchain – in Web of Science, 15.427 different results regarding the term were shown. Blockchain research has been performed since 2013 and has increased over the years, due to cryptocurrencies popularity, as presented in Figure 3.

The 15,427 results of the Web of Science search were classified into 191 different categories, where the top 10 with the most significant number of documents are presented in Table 1. In addition, documents were associated with multiple categories; hence the record counted being higher than the actual count.

By looking at the top 10 categories, there is a better understanding of the fields in which research has already been conducted. It is pretty clear, that this field of research has mainly been associated with computer science and telecommunication, with only a few entries by management and business.

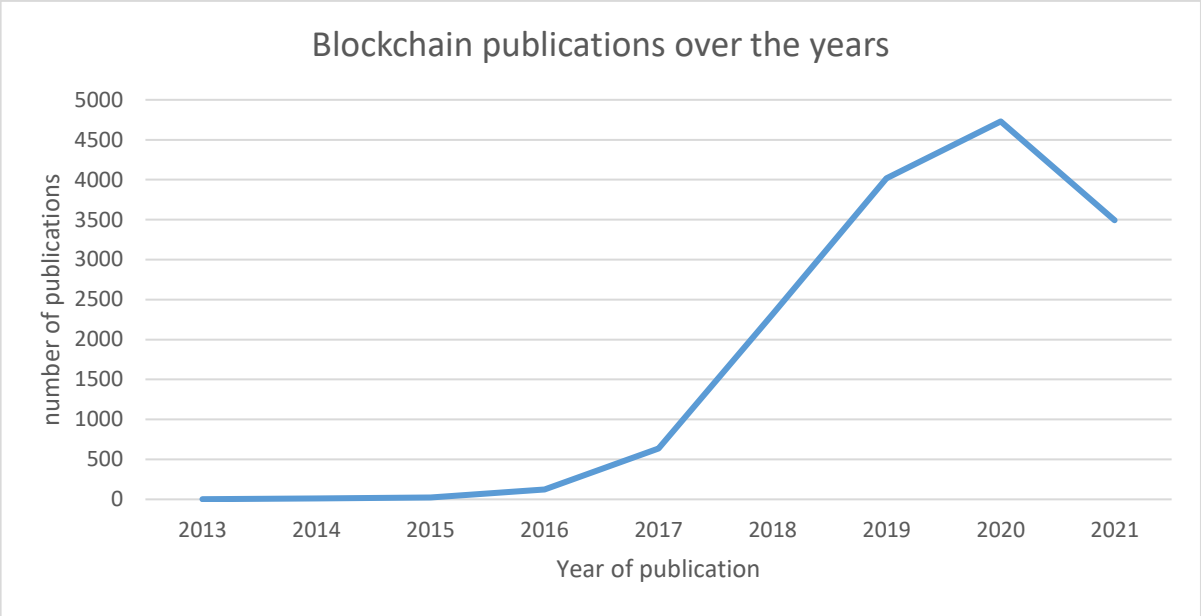


Figure 3: Blockchain publications over the years

Web of Science Categories	Record Count
Computer Science Information Systems	5587
Engineering Electrical Electronic	4480
Computer Science Theory Methods	4347
Telecommunications	4014
Computer Science Interdisciplinary Applications	1602
Computer Science Software Engineering	1279
Computer Science Hardware Architecture	1167
Computer Science Artificial Intelligence	980
Management	606
Business	486

Table 1 Top 10 Research Categories

When importing the data from Web of Science into VoSviewer, the number of occurrences that a term needed to be used – to be considered as relevant information – was set to 125. The visualization of the terms used in the documents and their connection to each other displayed a map that is presented in Figure 4. The map presented all the terms in five clusters, which are the grouping of terms that has a co-occurrence and their connection with the other terms.

The number established for the occurrences of a term – of 125 – could be considered as high, but due to the total amount of terms that were used being 172.928, it was required to reduce the number of terms – that were considered to be helpful to sort out the needed information. However, with such a high number of minimum occurrences, there is the possibility that some relevant terms are being excluded.

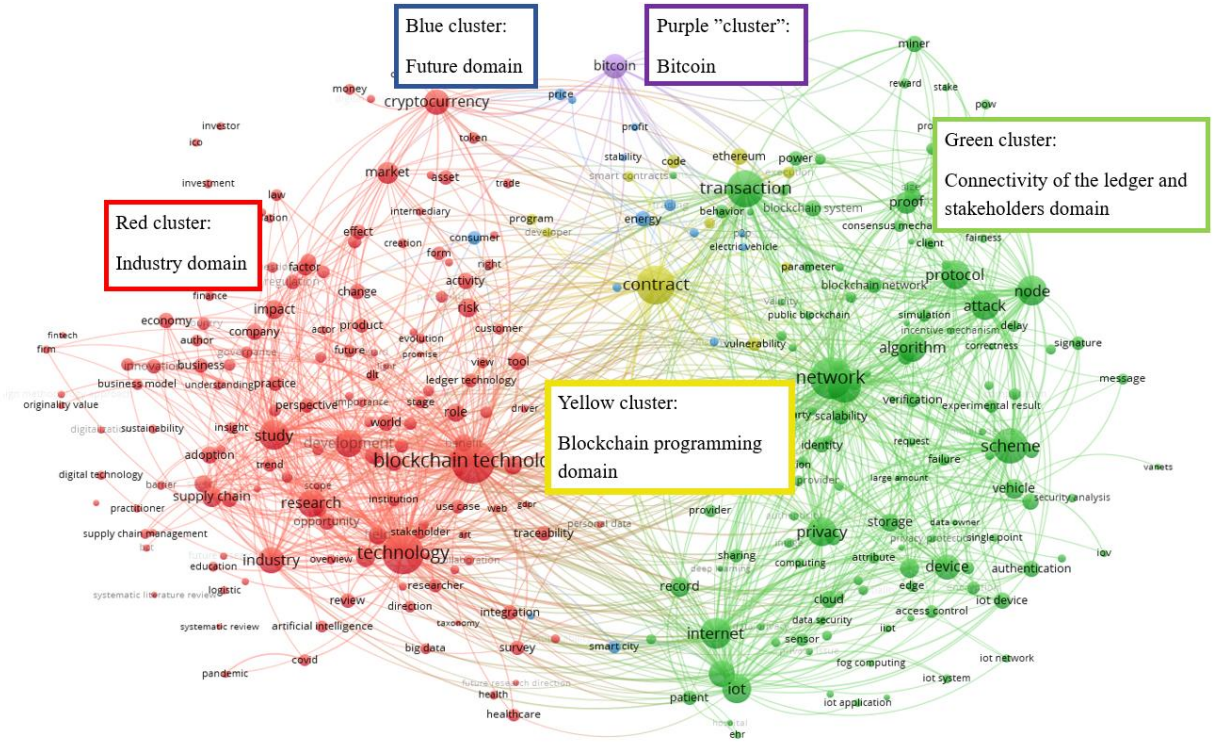


Figure 4 Broad cluster mapping

As it is shown in Figure 4, the largest cluster is the one in red where the focus of those researches was the industry domain. The most used terms in those documents were blockchain technology and technology, followed by other essential terms, such as cryptocurrency, investment, finance, development, and study. The second-largest cluster is coloured green, where the focus is the connectivity of the ledger and stakeholders. The most common terms were the internet of things, network, protocol, transaction, and authentication. Moreover, three small clusters were also visible in blue, yellow and purple. The blue cluster focused on the future and used terms like energy, smart city, electric vehicles, stability, and consumer. The yellow cluster focused on the blockchain programming domain made of the term associated with the construction of the ledger. The last cluster in purple contained only one term used: Bitcoin. Bitcoin is a cryptocurrency that is a term used in the red cluster, and even though it is only one term, it is still considered to be necessary since blockchains – as we know it – were created for this purpose.

As presented by the map in Figure 4, there is only limited use of terms that can be related to risks; these terms are risk, traceability, attack, privacy, and vulnerability. Most of these terms are not connected and are not used often. In the analysis of the map, clusters, and network, it was believed that a more specific search was needed to find the gaps that are associated with the connection of traceability, protection, risk, and user identification.

3.2 Specific analysis.

For the specific search, some conditions were added to the general term. By adjusting the search with the risk related terms, the result of the documents search was reduced to 69, instead of the 15.427 documents that were found at the beginning.

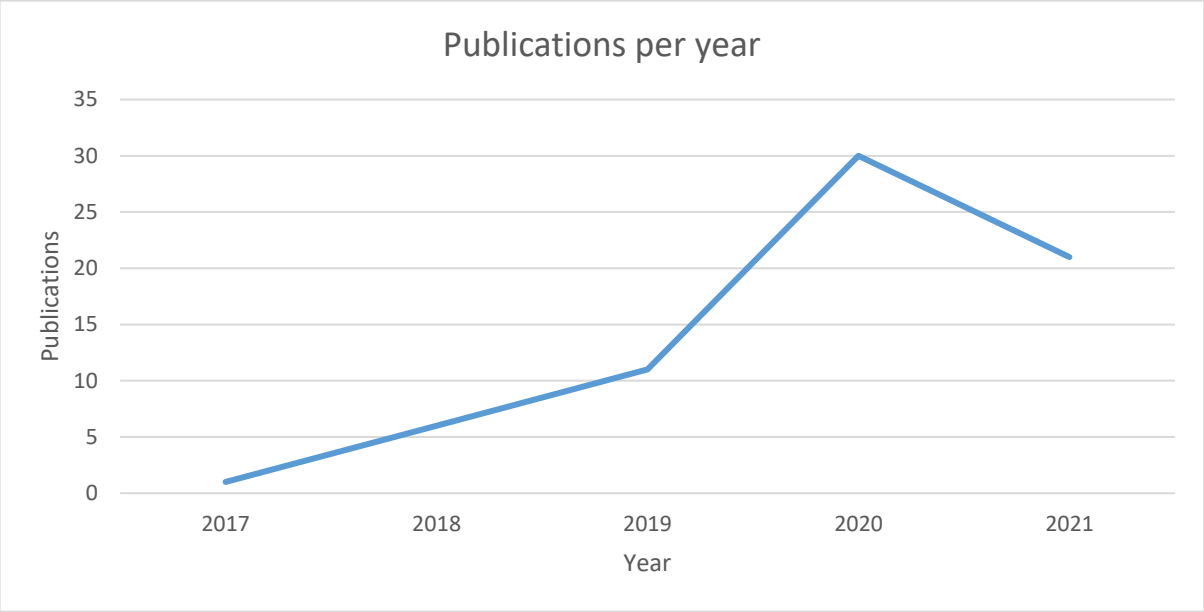


Figure 5 Publications per year related to the specific search

The risk related publications started later than the general research about blockchain technology, as appreciated in Figure 5. There has been an increase in research in this field, as seen in the increase of publications conducted each year. It was found that the documents were divided into 36 categories. The top 10 categories – with a chance that a document has been located in multiple categories – are as followed:

Web of Science Categories	Record Count
Computer Science Information Systems	26
Engineering Electrical Electronic	22
Telecommunications	21
Computer Science Theory Methods	10
Operations Research Management Science	6
Computer Science Software Engineering	5
Green Sustainable Science Technology	5
Physics Applied	5
Environmental Sciences	4
Management	4

Table 2 Categories related to specific search

In comparison to the results from the broad search, only the top two categories were located at the same place on the list. As reflected in Table 2, fewer computer science categories have been replaced by more industry-oriented categories. This could be an indication that the technology is getting more attention in the industry sector and an increase in the potential use of blockchain technology.

By mapping the documents, with the specification that a term needs a minimum occurrence of 10 and by selecting the 25 most relevant terms the cluster in Figure 6 was generated.

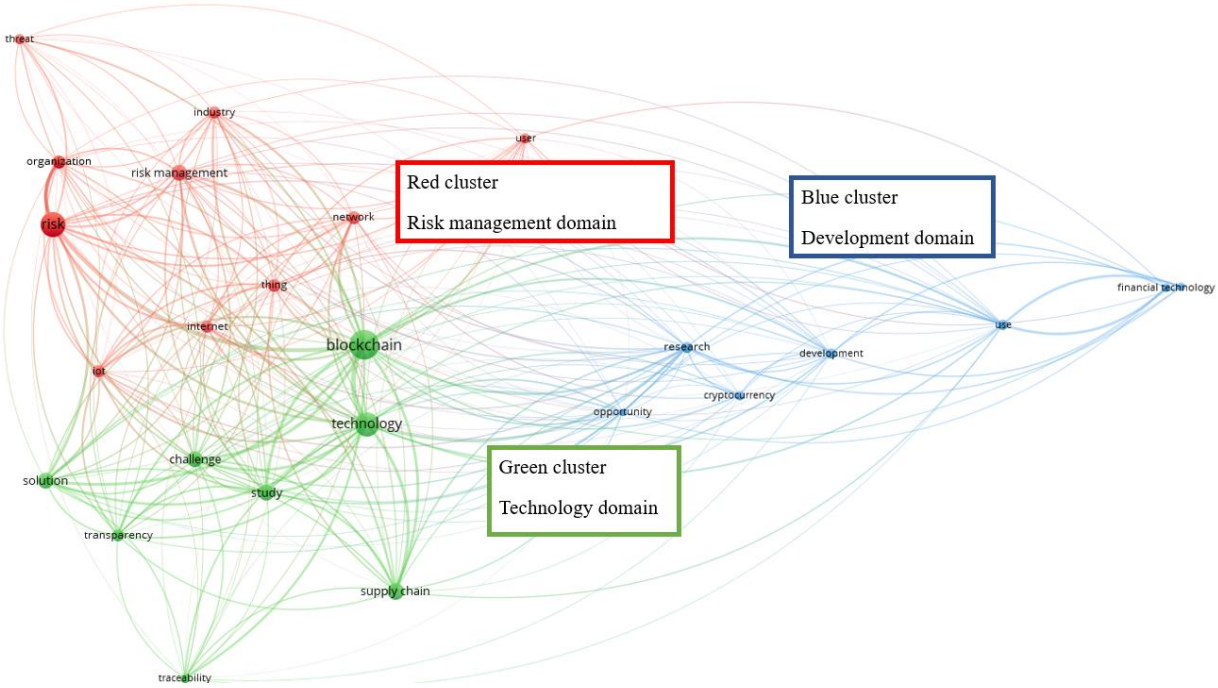


Figure 6 Risk-Related Mapping

The new mapping of the specific terms was divided into three clusters. The largest cluster is the red cluster, which has its focus on the risk management domain. In this cluster, the terms used were risk, risk management, threat, and user. The green cluster is related to the technology domain and contains words like technology, study, transparency, traceability, and challenge. Last, the blue cluster had the development domain, which contains finance technology, research, use, and cryptocurrency. The link between the terms has a low strength indicator, which helps to identify that the terms are not used often together. The visualization of the map and the strength of the connections show that little research has been done on the combinations of risk management processes and blockchain technology.

The 69 documents were then read to see how the terms were used. After looking through the documents, it was considered that only six was worth keeping for further reading. The documents were discarded based on how the author(s) used the terms, e.g. some used risk one or two times and when it was used, it was as a fancy word to make the document sound better. The selected documents were related to blockchain and risk management and could be able to

provide this project with relevant information. However, no documentation considered a similar angle – to be covered in this thesis; therefore, it is considered that there is a gap in the research already conducted and the applicability in the industry, which is taking a practical approach of how the risk management process and blockchain can be combined.

Blockchain technology can be seen as a new field in scientific research since the first documents started to cover the fields in 2013. The interest in the topic has only increased, with more research being conducted each year. Risk management and blockchain technology started scientific research in 2017, and the documents that have been produced are in low quantity, as of this thesis. The literature review analysis shows that there is a gap in the research in the field of risk management applications with the use of ledger technology as a basis for the RMP.

4 System Identification

This section will cover the systems that are identified as necessary for the development of the architecture. Therefore, a combination of three systems will be considered to create the risk management blockchain. The first system is the risk management process and how it is structured. The risk identification process that will be used as the basis for this thesis will also be explained in detail. The second system is the blockchain that is based on the characteristics of Ethereum. The last system is the public key infrastructure, which will provide the necessary characteristics for the proof of ownership and the security of the process participants. At last, the stakeholders that are involved in the RMP blockchain will be identified and their effect on the process will be categorised.

4.1 Risk Management Process

What is now known as risk management has been an evolutionary process that has had different connotations depending on the author. Likewise, some authors did not identify all the stages separately; for example, the International Electrotechnical Commission (IEC) in 1995 considered risk management as risk assessment and risk control, where risk assessment was seen as risk analysis and risk evaluation, as presented in Figure 7. For 2011, risk Management was considered as

> "a continuous management process with the objective to identify, analyze, and assess potential hazards in a system or related to an activity, and to identify and introduce risk control measures to eliminate or reduce potential harms to people, the environment, or other assets" (Rausand, 2011)

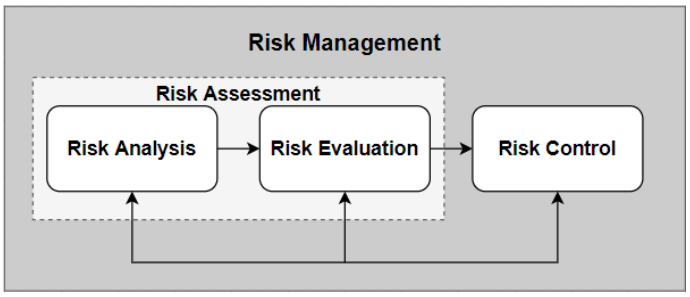


Figure 7 Risk Management Process inspired by IEC in 1995, based on (Rausand, 2011) and modified by the authors

According to the International Standardization Organization (ISO) 31000:2018, the risk management process aids decision making by accounting for the uncertainty and the possibility of future events and their effects (ISO 31000, 2018)

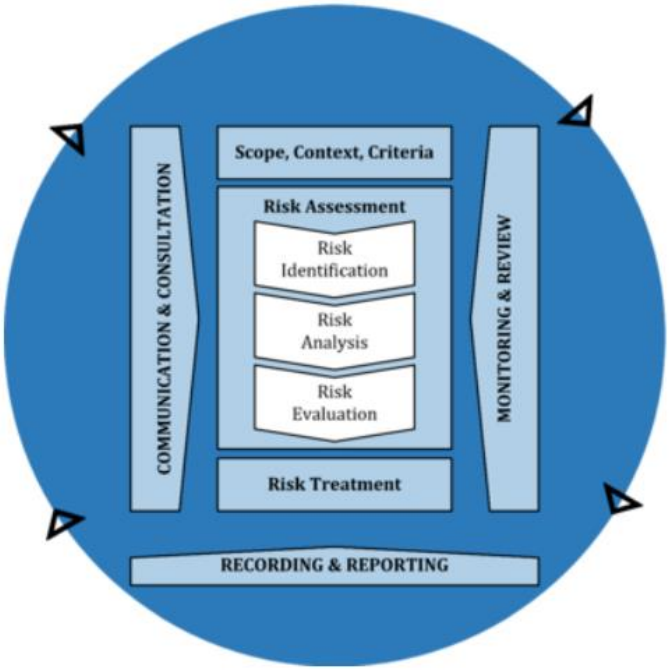


Figure 8 ISO 31000:2018 Risk Management process (ISO 31000, 2018)

The process, as presented in Figure 8, has six main parts. First, it starts with the definition of the scope; the second is the risk assessment, which is subdivided into risk identification, risk analysis and risk evaluation; the third part is risk treatment. The fourth and fifth parts are communication and monitoring, which are performed throughout the process. The last part is the reporting. Finally, the arrows indicate that this is a systematic process. This is the process that is proposed and used at the moment for some companies (ISO 31000, 2018).

4.1.1 Generic Risk Management Process

Although there are well known and recognizable processes for different authors and international institutions like ISO. For this thesis, a generic framework for risk management will be used. This process has five stages to be followed in order (as presented in Figure 9).

1. Risk Identification
2. Risk Estimation
3. Risk Evaluation
4. Risk Control
5. Risk Monitoring

and is complemented with risk communication through all the processes (Rangel, 2020).

Figure 9 Generic Risk Management Process (Rangel, 2020)

The process accounts for known stages to manage the risk, and it is structured with a systematic approach in each stage, that needs to be reviewed and accepted by the involved players. Each stage has steps to be followed, reviewed and accepted, before going to the next stage, and each stage has specific tasks to be fulfilled. Furthermore, is also thought in such a way that every shared information is transmitted by applying risk communication. The system starts with risk

identification and “ends” with risk monitoring; after that, everything needs to be managed again; thus, the process becomes recursive and starts again (Rangel, 2020). This process is not meant to be mandatory and needs to be adapted according to the project's necessities, business, resources, policy, location, etc.

An important connotation is that, even though a generic RMP will be used, when applied in a specific work, the internal structure of the stages could be modified depending on the project and the RM. This means that the steps and tasks could change since different methods could be applied, but what will be explained in this section will be applied for the rest of the thesis and the development of the architecture. As explained in section 1.4 Limitations, for this thesis, risk identification will be considered for the blockchain application and the architecture development. To see the complete RMP, refer to Figure 53 in appendix Generic Risk Management Process. Therefore, the risk identification process will be explained next.

Risk Identification

Risk identification is the first stage of RMP where a problem is identified and is associated with a risk that needs management; hence it is necessary to obtain information. Therefore, it is necessary to perform a first recognition of the problem by performing the following tasks:

- Definition of triggers and inputs
- Identification of triggers and inputs
- Identification of consequences or the sequence of events
- Identification of uncertainties

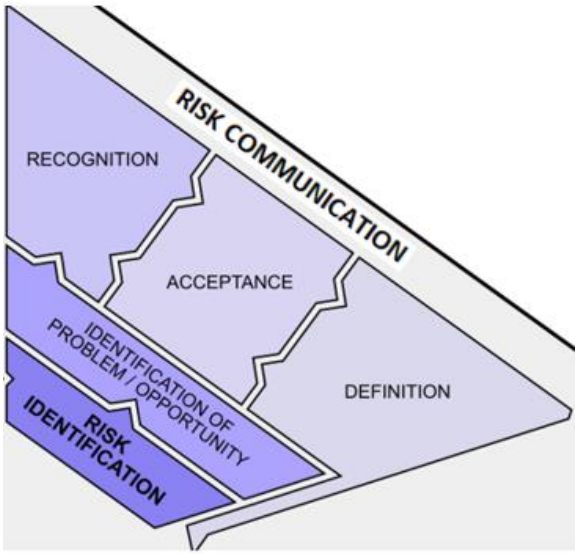


Figure 10 Risk Identification Steps (Rangel, 2020)

From this broad identification, the process of risk identification starts and could be structured in four recursive steps, as presented in Figure 10. These steps will make it available to gather

the "right" information, to present and communicate the problem statement in terms of the identified (Rangel, 2020).

1. Identification of Problem/Opportunity

The problem/opportunity step aims to find everything that represents a problem for the system and everything that could be considered an opportunity. For this, it is necessary to redefine the previous identification to make it understandable to be socialized; therefore the following five tasks are required to be performed (Rangel, 2020):

- Identification of the inputs and triggers events
- Identification of the hazards and opportunities
- Identification of harms and gains related to the hazards & opportunities
- Identification of the sequence of events for hazards & opportunities related to harms & gains
- Identification of uncertainties related to the sequence of events, harms & gains, and hazards & opportunities

At this step, some tools for risk identification, consequence assessment, and uncertainty characterization could be applied and could be repeated until "everything" covers the possible problem.

2. Recognition

The recognition step aims to understand and select the problem – considering all the perspectives, thus framing the problem in an understandable and precise way. Therefore, frame analysis is necessary, to socialize and promote the participation and contribution of the actors with their problem definition. The purpose of this analysis is to avoid misunderstandings, obtain the correct problem/contribute to the diagnosis and definition (Rangel, 2020). For this case, the frame analysis tasks will consider eight practices (Rangel, 2020; Wedell-Wedellsborg, 2017):

- Establish legitimacy of the framing as a method for problem identification
- Find participants and outsiders to bring them into the discussion
- Get the problem definition written from each participant
- Ask and analyse what is missing in the definitions
- Find the structure: categorize, associate and classify the thoughts of the group
- Analyse constraints: positive and negative exceptions; situation and states where constraints may occur
- Analyse and question the objectives and current knowledge

- Explore other frames and/or re-iterate the previous process

This step could be repeated to contemplate different frames where only one will be chosen to be presented as a *Problem frame analysis* document, in order to be delivered and reviewed in the next step.

3. Acceptance

The acceptance step aims to have the acknowledgement of the problem, the willingness to do something about it and the ability to address the problem when the resources and planning have been foreseen (Rangel, 2020). Some of the needed tasks could be – but not limited – the following:

- Acceptance and willingness to solve the problem from the manager
- Acceptance and planning for allocation of resources

The deliverable from this step is a *Problem acceptance* document that must include the planning.

4. Definition

The definition is the last step of the risk identification stage. Once the problem had been understood – recognised and accepted – then it is necessary to define it in terms of risk communication. Therefore, a problem definition process must be performed; this could be according to the project's necessities and should be used the most favourable. Some of the tasks of this step are the following:

- To choose a problem definition process
- To perform the problem definition process or processes
- To collect and combine the data from the process
- To define the problem, all the findings that will be addressed

The result from this step and the risk identification stage is the *Problem statement* document. This will determine the final risks that will be addressed in the following stages of RMP.

The same step and task approach apply to the other stages of the RMP. It should also be noted that the approach described above could change according to the needs of a project, the methods, processes, etc., that the risk manager (RM) uses to obtain better results. As previously stated, it is a generic process that will be used to propose the architecture of the process in the blockchain, which will serve as the basis for the development of the complete RMP.

4.2 Blockchain

In the following part, the principle of how blockchain technology is designed and how it works will be described. Blockchain technology contains multiple different technologies that are used to function. The first blockchain was proposed from the white paper presented by Nakamoto; this was the first protocol that was made for the cryptocurrency Bitcoin. Over time, more protocols have been created due to how the creator of a blockchain would like the specific chain to function. The most common protocol used in the industry sector is Ethereum. Ethereum can utilize smart contracts, a feature that makes it more desirable for companies.

To understand how this all works, an explanation of the structure is needed — first the blockchain, which functions in three layers, the protocol, the blockchain technology, and the token and then the different network types.

4.2.1 Protocol

The first thing to consider when creating a blockchain is what protocol to use. The blockchain can be developed with different intentions, and therefore protocols could present different guidelines and rules to function. This is also how the data validation of a block is set, known as the consensus protocol. The two best-known protocols are Bitcoin and Ethereum (Genesis Devcon, 2018), which have created different protocols that are more suited for the design purpose. For this thesis, the protocol used is the Ethereum protocol because it is open-source and has created an enterprise protocol that gives the companies total control of the chain (Gwyneth, 2021). The description of blockchain technology will therefore be based on the Ethereum protocol.

The consensus protocols

The choice of consensus protocols is to ensure that the blockchain system operations are stable. This is due to an agreed method for adding a block to the chain. When selecting the consensus protocol, two main methods are used the most and other methods have made alternations from the main protocols. The main protocols are Proof-Of-Work (PoW) and Proof-Of-Stake (PoS) (Kim et al., 2020; S. Zhang & Lee, 2020).

PoW is where everyone who can access the blockchain can mine new blocks. The puzzle they are trying to solve is of great difficulty, and the miners will have to change the nonce multiple times to find the targeted hash. This big competition method rewards the first user for generating the targeted Hash (S. Zhang & Lee, 2020).

PoS is where everyone who can access the blockchain can validate new blocks by putting something on the stake. In the first PoS method, a user puts currency on the stake – greater than the transaction – for being selected as a validator. The selection of a validator is chosen at random, but if a user puts a larger amount of currency on the stake, they increase their probability to be selected and gaining more fees. The validator can lose what is at stake if the user is not redeemed as a reliable validator. Other methods have been developed with

alternation – e.g. Proof-of-Burn, Proof-of-Authority – but they are all based on a validator having to stake something to be trusted in the network.

4.2.2 Blockchain technology

The technology stores records of transactions in a ledger structure. The storing method can be considered as a *block*. The blocks are linked together and create a chain, hence the name blockchain. When a block is being added, three categories of parameters need to be fulfilled to validate that the block is correct and safe to add. These three categories are account state, transactions, and the block (Dr Wood, 2021).

Account State

The account state refers to the sender of data and contains four factors: $Nonce_{account}$, *balance, storageRoot, and codeHash* (Dr Wood, 2021).

- The $nonce_{account}$ is a value that is associated with the number of transactions that comes from an account
- The balance is a value that indicates the value of the currency on the account
- The storageRoot is a 256-bit hash that encrypts the account and hides how much is stored on the account
- The codeHash is the code string that is generated based on all the named parameters above. This codeHash cannot be changed after the state have been created

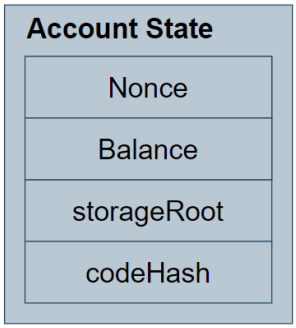


Figure 11 Visualization of Account State

Transaction

The transaction – as the name implies – is an interaction between two accounts where one is sending data to another. A transaction consists of a $nonce_{transaction}$, *gasPrice, gasLimit*, *address, value*, and *signature* (Dr Wood, 2021).

- The $nonce_{transaction}$ is still a validation number
- The gasPrice is the amount that is going to be paid for creating the transactions
- The gasLimit is the maximum amount of gas that can be used for the transaction

- The Address is the receivers address that is needed for sending the information
- The Value is showing the amount that is being transferred
- The signature(v,r,s) is used to notify that it is the rightful person that is making the transfer. The signature is based on ECDSA

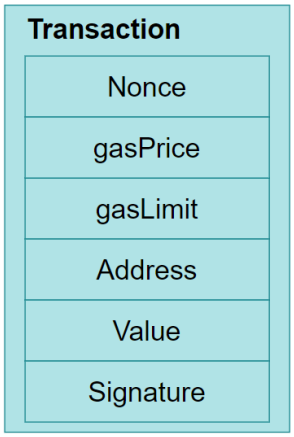


Figure 12 Visualizations of the transaction

Block

The block is the collection of all the relevant information for creating a block and which correspond to the transactions. The block – known as the *blockHeader* – shows all the available information for the public on the ledger. The blockHeader consist of *parentHash*, *ommersHash*, *beneficiary*, *stateRoot*, *transactionsRoot*, *reciptsRoot*, *logsBloom*, *difficulty*, *number*, *gasLimit*, *gasUsed*, *timestamp*, *extraData*, *mixHash*, and $Nonce_{block}$ (Dr Wood, 2021).

- The parentHash is the hash of the previous block
- The ommersHash – uncleHash – is the hash of the parentHash sibling. Meaning that if two blocks are validated at the same time, they both cannot be added to the main chain, hence creating a fork. Therefore a list is kept of the hashes that have not been added to the main chain. The list keeps blocks for six generations that can be added later to reward the miners of the ommerHash
- The beneficiary is the address of the miner who successfully created the mixHash and shows where the fees shall be sent to
- The stateRoot is the hash created when all the transactions in the block have been executed and applied. It is an indicator that verifies that the accounts have the amount that they are sending
- The transactionsRoot is a hash that is generated based on a list of all the transactions, verifying that they are all correct
- The reciptsRoot is a hash that is generated for every receipt in the transactions.

- The logsBloom is a filter that stores all the information gained from the receipts, based on the transaction list. It creates an index list that makes it possible to search for a specific transaction in a block
- The difficulty is a factor for deeming how fast a block can be mined. The greater difficulty, the longer time or more computer power it will take to validate the block. This is an automated process based on the protocol's creator
- The number is the value in the chain. The genesis block starts with 0 and the number after the genesis block can be seen as "Block N+1", where N is the number of the previous block
- The gasLimit is shown per block as the limit expenditure for the block
- The gasUsed shows how much gas has been used for mining all the transactions
- The timestamp is the time measured in Unix's time. Unix's is a timer that shows how many seconds have gone since 1/1-1970
- The ExtraData could be if additional data is needed in that specific block. It is, however, limited to 32 bytes
- The $nonce_{block}$ is a 64-bit value that is made for the validation of the block combined with the mixHash
- The MixHash – is combined with the Nonce – is a 256-bit hash that is used for validation of the block. The mixHash can be seen as the block hash

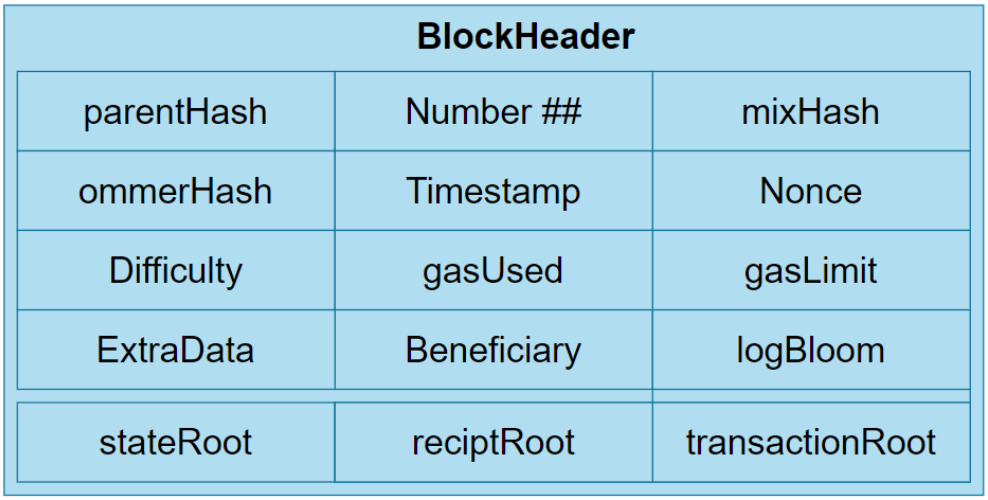


Figure 13 Visualizations of the Blockheader

mixHash calculation

With the components of the blockchain that have been described, the following section will give a more detailed explanation of some of the different functions and how these can interact with each other.

Hash

It is necessary to understand what a hash is since this is one of the biggest securities features that blockchain provides and one of the main components in understanding why the technology works. The hash is an encrypted method that all blockchains are using to secure the information in the chain. The message is encrypted by the *SHA-256* functions, which stand for Secure Hash Algorithm using 256-bit encryption. Ethereum is using *Keccak-256* which is a third-generation SHA system – SHA3. When using SHA3-256 for encryption it transforms information into an unreadable string of code, that cannot be reversed engineered – as of this thesis – unless one has the corresponding key. The reason why SHA3-256 is used is because of the high level of protection it provides (Dr Wood, 2021).

The SHA3-256 is one-way only and is considered to be almost impossible to reconstruct the original information after it has been encrypted. If an attacker wants to decrypt the code by using a brute-force attack, which is simply guessing the right combination, the number of attempts that would be needed is 2^{256} to get the initial information. Second, the probability that the same hash will appear twice in the same chain – this is called a collision – is almost non-existing. The number of brute-force guesses that needs to be done would be $2^{N/2}$, where N is the number of bits. With the SHA3-256 being able to create 2^{256} possible outcomes, that number would be reduced to $2^{128,}$ which is still a number so large that humans cannot imagine it (Penard & Werkhoven, 2007).

For calculating the hash, the SHA3-256 can be seen as a function that works in three steps. Step one is the part where the data is given a length of a code string. The SHA3 have a length of 1600 bits, and the data goes through a 5x5 algorithm, 24 times. In step two, the first encryption string is divided into smaller pieces, and all these pieces are calculated 24 times. In the end, the calculated string consists of 1600 bits. In step three, the data is finalised and compressed in a string consisting of the 256-bits, that the SHA3-256 uses. The 256-bits are chosen based on the first bits of the output string (Anand, 2019; Team Kaccak, 2021).

Roots

The Roots is the data that is shared, and the steps in calculating the hashes are shaped like a tree – the Merkle-Patricia tree (Dr Wood, 2021). Figure 14 presents how the hashes are developed. The Merkle-Patricia tree contains three groups that combined results in the single *rootHash*, *Leaf node* (green), *extension nodes* (light brown), and *branch node* (brown). Leaf and extension node consists of two things, a key and a hash. The branch node 17 items, were 16 of that correspond to the key value, which can have 16 possible values, 0-9 and a-f. The last item is used if it is a terminator node (Dr Wood, 2021).

The leaf node contains the data that is being encrypted. The encrypted data is then converted into the extension node. Two extension nodes are then combined into one extension node, and this process is continued until only one node is left, the rootHash. In case of a multiple collision where multiple keys start with the same number, the branch node is used to divide the extension

node into groups, making them viable in the Merkle-Patricia tree. The function of the roots is to validate if the transactions are reliable and correct (Dr Wood, 2021). The Root function is the same method that is used for reciptsRoot, transactionRoot, and stateRoot.

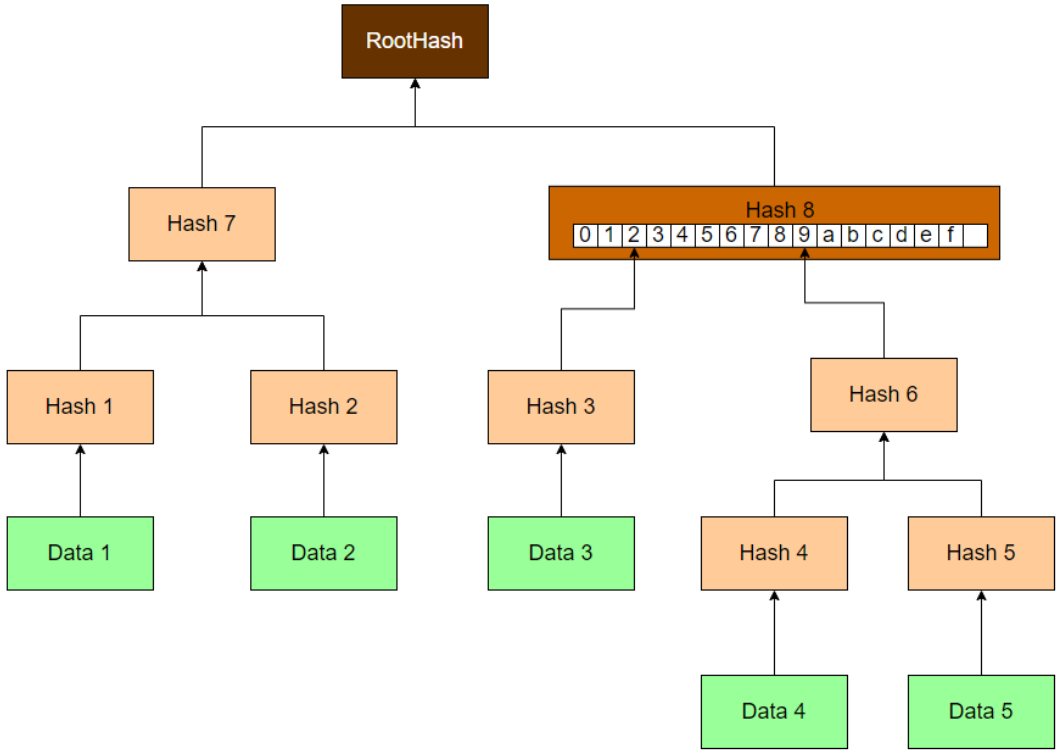


Figure 14 Modified Merkle-Patricia Tree

Nonce

The nonce is a 64-bit unsigned number that is part of the hash generating in all parts of the block and is part of the PoW (Dr Wood, 2021). The number of an unsigned integer is ranging from 0 - 2^{64}. The nonce helps to find a specific hash, by changing its number the mixHash is changed.

Proof of work

The nonce can be seen as a hash modifier that can be used to get the hash, to reach a value with the specific criteria. If more users join the chain, then the hashrate – a term used for determining how many hashes can be calculated per second – will increase, making it faster to add blocks to the chain. The increased hashrate, trigger the protocol to change the difficulty thus it fits the target time (Kim et al., 2020). Figure 15 presents, how the mixHash is calculated. When the calculation process is computing the only changes are the nonce and the time. For every second that passes the nonce changes multiple times to find the mixHash. The miner can start from nonce = zero and go through as many nonces as possible before that second have passed and the next starts. If a miner finds the nonce that matches the mixHash with the target the difficulty, the PoW is completed; if not, then the miner can start from zero again. This process is repeated.

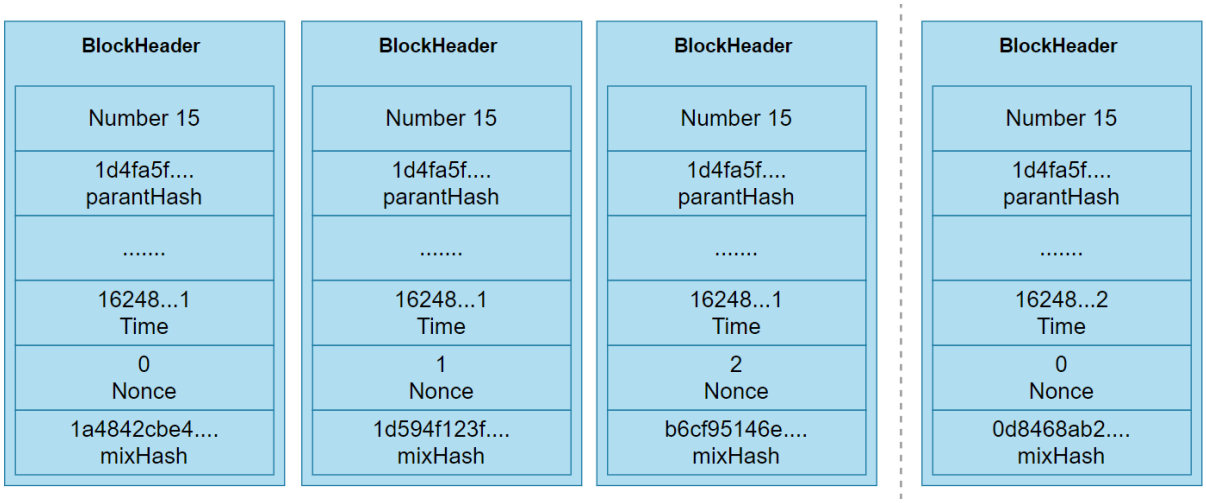


Figure 15 Simplified mixHash Calculation

Concepts of the technology

Immutable ledger

When the hash has been calculated, the block is added to the chain. When blocks are added to the chain, the block's location is consistent and continuous. It is impossible to add or replace a block in the chain other than the next block in line. Figure 16 presents how a chain and where the next block is added. This increases the security of the chain since all the blocks are connected by the mixHashes and give the block a specific place in the chain. If they were to be replaced, this would disrupt the mixHash connections and invalidate the chain. To change a block or add a block, one would have to change the whole ledger from the point where it was put in. This is done to prevent attackers provide wrong or harmful data to the chain. In the case where two blocks are validated at the same time, a fork is created. A fork is unwanted because it complicates how blocks are added. When this happens, the first block is added to the main chain, and the other block becomes an ommerblock. The ommerblock is then added as extra security for the following main block (Van Hijfte, 2020).

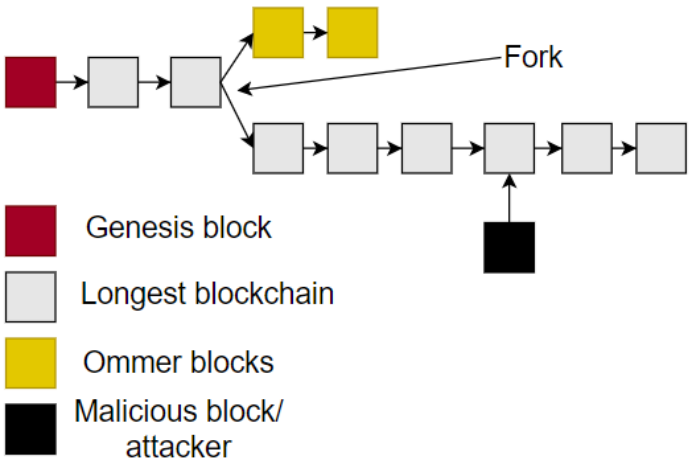


Figure 16 Blockchain visualized

Smart contracts

A smart contract is a program that can be uploaded to a blockchain, which can execute specific operations if certain criteria are fulfilled. The idea is that this function will occur automatically without any external interaction (Kim et al., 2020).

Scalability

To make a blockchain function, there is a need for taking scalability into account. What is meant with scalability is that when the blockchain gets longer, the resources needed to operate increase. If the amount of storage required for the blockchain increases, the validation's time is prolonged, the currency's value decrease, the fee's cost increases, and it makes the synchronization's time longer. The scalability shall be considered in the protocol to make sure that the blockchain does not stop functioning in the future (Dr. Wood, 2021; Kim et al., 2020).

Transparency and privacy

One of the essential concepts of blockchain is openness and closeness. By making every transaction public, everyone can see what is being exchanged. The purpose of this is to make it harder to cheat since the currency can be tracked. However, the accounts are still private, so it is impossible to see who the sender or who the receiver is, only the public address is visible (Nakamoto, 2008).

Wallet

To exchange data on a blockchain, a person needs to have a wallet. A wallet is used to store information of a person, which could be currency or credentials. For a person to access his/her private wallet, they would need to have one key called a *private key*. A private key can be used to generate a *public key*, which can be seen as an address linked to the private key. A private key can generate as many public keys as the owner wants to keep their privacy. Since the system is decentralized, if the person loses access to their private key, there is no other way to recover the wallet (Kim et al., 2020).

4.2.3 Token

A token – which can be seen as a coin – is part of a cryptocurrency that a specific blockchain uses. The function of a token could be as a currency that can buy items similar to the current monetary system like Euros, Dollars, etc. They could also be used for investments, funding, storage, or what the creator wants (Frankenfield, 2021).

4.2.4 Networks

Peer-to-peer network

A blockchain is a distributed ledger where everyone who wants to access it can connect to the chain. When a user connects to the ledger, it begins to download the whole blockchain, which is used as a reference for future blocks. When users have accessed the blockchain, they become

part of a peer-to-peer network and are part of the validation process. This means, before a block can be added to the chain, the majority of the users have to reach a consensus that the block is next. This is the process that makes blockchain technology decentralized. Because every transaction has to reach a consensus with the majority of the users, it removes the need for a central authority to validate the transactions. (Badratdinov, 2018)

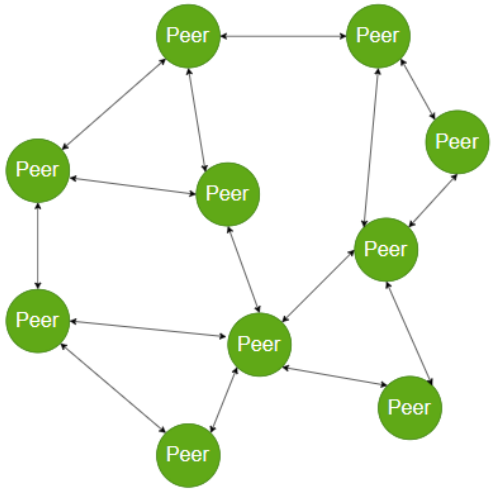


Figure 17 Peer-to-Peer network

A blockchain can use three types of networks – *public*, *private*, and *consortium* networks (Kim et al., 2020).

The public network is the first system presented by Nakamoto. It functions by everyone having access to the ledger and being part of the transactions, either mining the blocks or making transactions. This is the network used for cryptocurrency, such as Bitcoin, Ether, etc.

The Private network is fully controlled by a centralized authority. They have complete control over who has access to the network and who can contribute to the transactions and the mining process. The protocol is made up based on the values of the organisation. This is the type that is more suited for enterprises and governments.

The consortium network is the system that mixes the private and public. The focus is to make better interactions between different groups controlled by a group(s) on the network. This type is suited for collaboration between different companies.

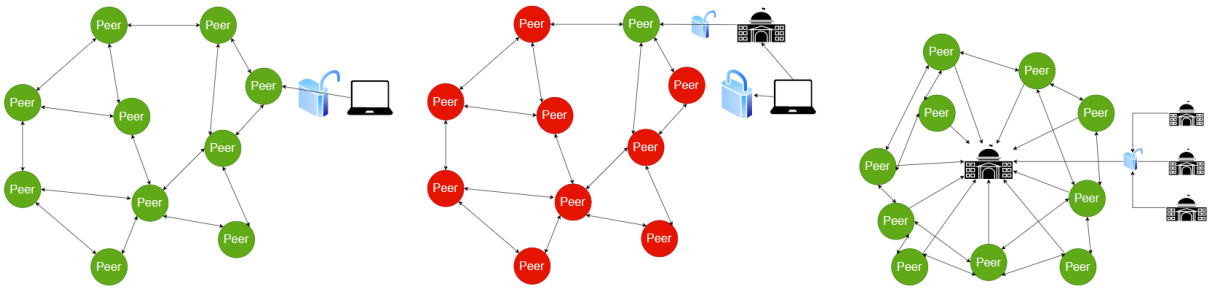


Figure 18 Blockchain Networks, From the left Public, Private, Consortium network

4.3 Public Key Infrastructure

This section intends to introduce the system that will be combined with the blockchain in order to authenticate the people and their work. Therefore, this section will explain what a public key infrastructure (PKI) is, what it consists of, the technologies it could use and some basic knowledge necessary to create the desirable public key infrastructure.

A PKI is a set of technologies and procedures that provides security through the use of cryptography (Trcek, 2014; Vacca, 2004). PKI allows public network users to exchange data securely and/or privately by using two encrypted keys – a public and a private. These keys are obtained and shared through a trusted authority that provides digital certificates; these certificates authenticate the identity of the persons (Vacca, 2004).

4.3.1 Keys

The key concept is related to cryptography, where the idea is to encrypt plaintext into ciphertext through a cryptographic algorithm.

Key Pair

The key pair provides two related but different keys that cannot be derived or computed from each other, even by knowing one of the keys. Therefore, one of these keys can be publicly available – *public key* – while the other remains secret – *private key*. The idea of making a key accessible to the public created the *public key cryptography* concept, which has produced several services available, one of these is the PKI (Adams et al., 2003).

Key Generation

The keys' generation could be done in two ways – *symmetric* or *asymmetric*. The symmetric keys are generated with quality pseudorandom generators. The asymmetric keys are determined by specialized cryptographic algorithms like the ECDSA used in blockchain (Trcek, 2014).

4.3.2 PKI Entities

For the keys to work in a PKI system, it is necessary to explain what entities are required to operate certificates and verify people related to a public key. The interaction between the entities is presented in Figure 19, and PKI entities are:

- **Certification authority** (CA) is the entity that issues, verifies, distribute, renew, revocate and suspends the digital certificates (Ariwa & El-Qawasmeh, 2011; Vacca, 2004)
- **Registration authority** (RA) is an optional local agent that verifies that all procedures and requirements were followed according to the policies before a digital certificate is issued Also, it verifies the authenticity of the subscriber to issue a certification to the CA. (Ariwa & El-Qawasmeh, 2011; Vacca, 2004)

- **Subscriber** or a certified user is a person or entity that has been issued a certificate (Vacca, 2004)
- **Relying Party** is the user that receives the digitally signed information from the subscriber (Vacca, 2004)
- **Certificate Revocation Lists** (CRLs) is a time-stamped list that identified revoked certificates (Ariwa & El-Qawasmeh, 2011)
- **Certificate Repositories** is a system or distributes systems where the certificates will be stored and from where the certificates will be distributed (Ariwa & El-Qawasmeh, 2011; Vacca, 2004)

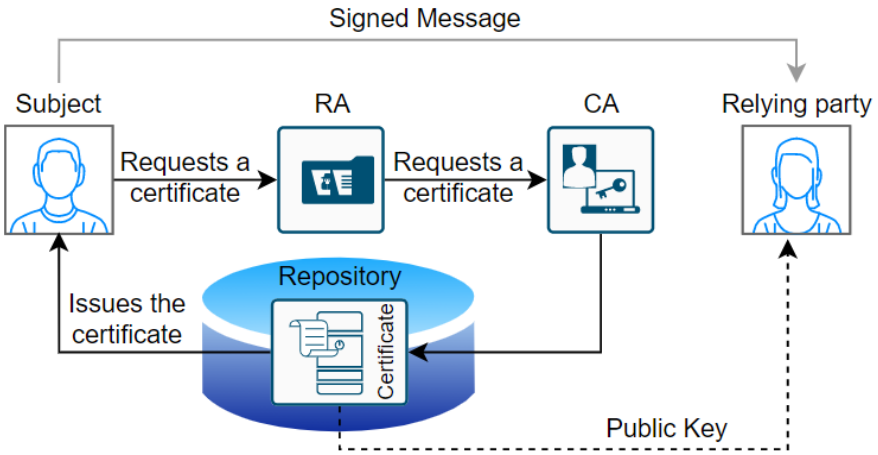


Figure 19 Entities and Operations inspired by (Binder, 2002)

4.3.3 Certification

The fundamental function of PKI is to certify that the public key belongs to a specific subscriber. Hence, a certification provides "a secure way of publishing keys, so that their validity can be trusted" (Binder, 2002; Vacca, 2004).

To provide a valid public key to a third party, a certificate will come with the key, as presented in Figure 20. The certificate will contain at least the basic information of the subscriber, this could be – but not limited to: the subject identification information, subject public key, CA identification information, and validity. In this way, a true certificate will prove that the available public key belongs to a specific subscriber, can trust the identity of the public key, and may be used by other subjects (Binder, 2002).

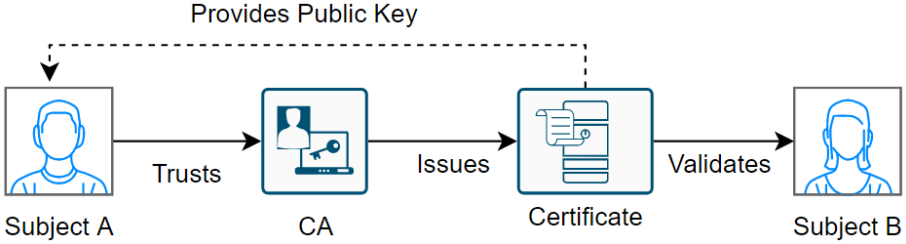


Figure 20 Certificate inspired by (Binder, 2002)

Cross certification

The certification could be done by one CA, but not everybody trusts the same CA. Therefore, a cross-certification could be applied. Cross certification involved two CAs that trust each other and create a pair of cross-certificate that will validate each other (Binder, 2002). The process is presented in Figure 21.

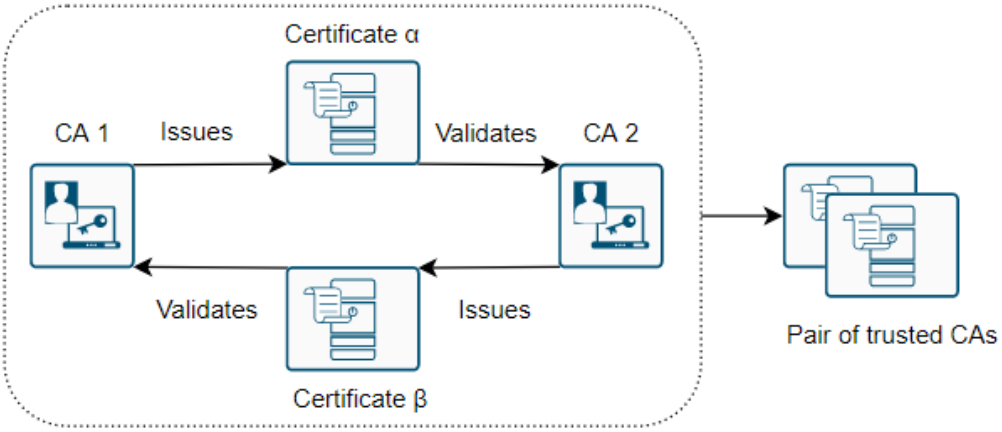


Figure 21 Cross certificates inspired by (Binder, 2002)

Certification path validation

To certify and validate a public key where several CAs exists, a number of CAs must validate each other – even though not all CAs could be connected via cross-certification – until a certificate is obtained. (Binder, 2002) As presented in Figure 22.

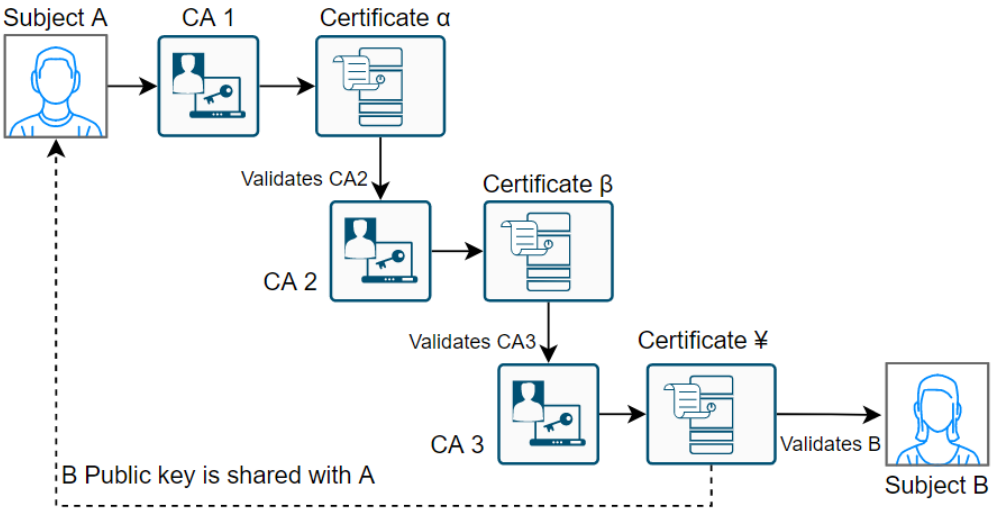


Figure 22 Certification path validation process inspired by (Binder, 2002)

CA relationship of PKI

In a PKI, CA relationships are scalable. Therefore, depending on the general relationships between their subjects, the CAs can be organized in three ways:

1. *General hierarchy* is where each CA certifies their parents and children. In addition, a link between CAs could happen by additional cross-certificates (Binder, 2002). As presented in Figure 23, where double arrows represent the possibility of cross-certificates.

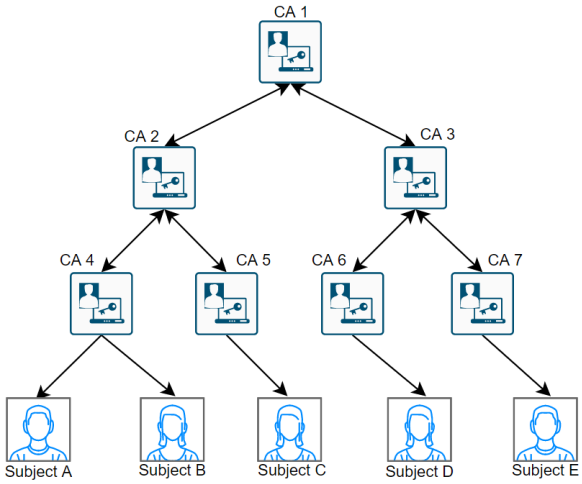


Figure 23 General hierarchy with cross-certificates inspired by (Binder, 2002)

2. *Top-down hierarchy* is when all users must trust and use the top-level CA as their root CA. Also, each top-level CA certifies only its children. Therefore to use PKI, all users must have a copy of the top-level CA public key (Binder, 2002). As presented in Figure 24.

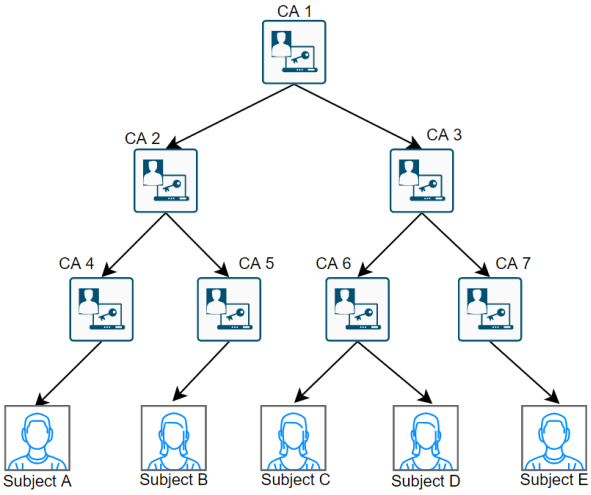


Figure 24 Top-down hierarchy inspired by (Binder, 2002)

3. *Web of trust* occurs when the CA bases its trust on the certificates of other CAs since these certificates depend exclusively on the cross path. In addition, users exchange keys and sign each other's keys to establish trust (Binder, 2002).

Validation

The validation ensures that the certificate information is valid. This is performed as the certification path validation. For this, either the user asks about the validity of a certificate to the CA or the CA could include a validity period in the certificate – this is known as offline validation (Binder, 2002).

Revocation

It is a process that is carried out when the information in a certificate becomes invalid due to a change in basic information, damaged information or stolen information. Therefore, the CRL should issue a list of revoked certificates and contact the user (Binder, 2002).

Authentication

The authentication is done for the public key; for this, one of three things is required – something that the user knows, something that the user possesses or something the user is (Binder, 2002).

- Knows: could be a password or a shared secret
- Possession: is a physical token like a proximity card, smartcard, visa card, ID, etc. and is usually combined with something the user knows
- Is: biometrics (fingerprints, retina scan) or DNA

4.3.4 Technologies

There are different kinds of technologies that could be used for the PKI. Some are the following:

Symmetric encryption

Symmetric encryption is the classical form of cryptography, also known as the secret key. The same key is used for the encryption of plaintext and the decryption of the ciphertext, as presented in Figure 25. The main advantage is that it can be efficiently implemented in computing environments. The main disadvantages are the complex key management – the number of secret keys needed per participant to communicate is proportional to n^2 – and the insecure transporting of the key (Trcek, 2014; Vacca, 2004).

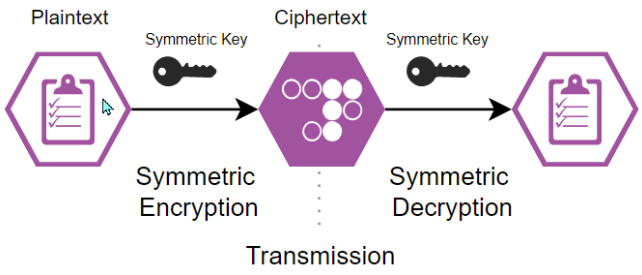


Figure 25 Symmetric encryption inspired by (Binder, 2002)

Asymmetric encryption

Asymmetric encryption is also known as public-key cryptosystems, is a process that uses two complementary keys, one private (secret) and one public, for cryptography transformation. A public key is used to encrypt a plaintext that needs to be sent, and this new ciphertext can only be decrypted by the complementary private key to reveal the original plaintext (Trcek, 2014; Vacca, 2004). This is presented in Figure 26.

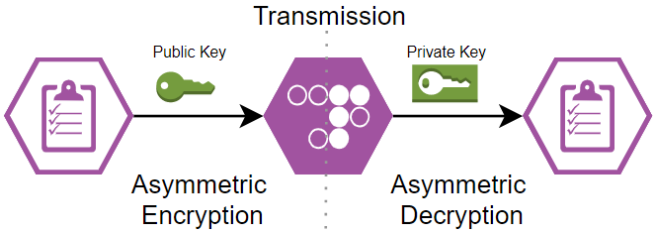


Figure 26 Asymmetric Encryption inspired by (Binder, 2002)

One way Hash Functions

One way Hash Functions is a cryptographic method that takes an input and produces a hash (Trcek, 2014). This means that the method is used to obtain a unique "digital fingerprint" from specific data (Binder, 2002), as presented in Figure 27. This method aims to provide integrity to the shared data by proving that the original data has not been modified.

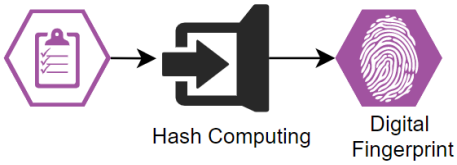


Figure 27 One way hash function inspired by (Binder, 2002)

Digital signature

The digital signature is a combination of asymmetric encryption and hash, where specific data need to have a digital signature. The following process is presented in Figure 28 for the digital signature creation,

(1) the plaintext needs to be hash which will create a digital fingerprint that will need (2) to be encrypted with a public key to get the digital signature. Once the signature is generated, (3) it has to be combined with the plaintext (not hash), meaning that the data is now signed. This will provide integrity and non-repudiation to the plaintext and is ready (4) to be shared (Binder, 2002; Vacca, 2004).

Once the signed plaintext has been transferred and received:

(5) the plaintext and the digital signature are separated. The signature (6) will be decrypted with the complementary private key, and (7) the plaintext is hashed in a temporary digital fingerprint. This hash and the digital fingerprint (8) are compared, and if they match, it authenticates the signed plaintext (Binder, 2002; Vacca, 2004).

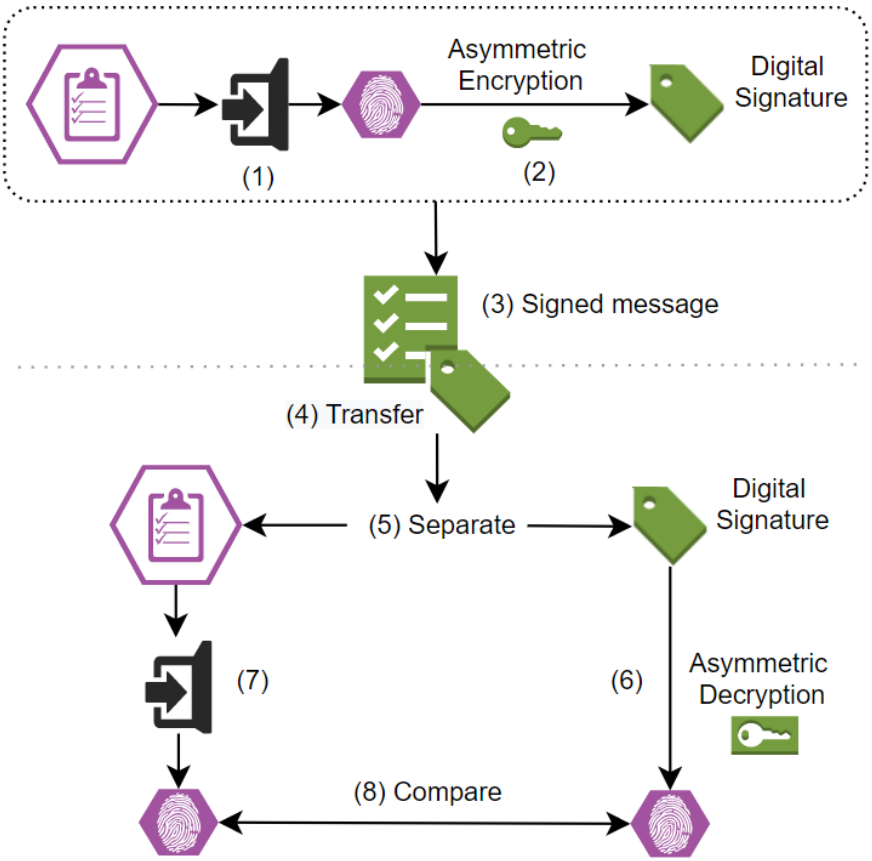


Figure 28 Digital signature inspired by (Binder, 2002)

Digital signature associated with message encryption

The digital signature associated with message encryption is a method where a signed plaintext could be shared in a confidential mode; therefore, additional steps must be taken, as illustrated in Figure 29.

(1) The plaintext is encrypted with a symmetric random key, (2) then this random key is encrypted with a public key. (3) The now encrypted key, the digital signature and the ciphertext is combined (4) to be shared (Binder, 2002; Vacca, 2004).

Once the package is received:

(5) The ciphertext, the random key and the digital signature are separated. (6) The decryption of the random key will be possible with the corresponding private key. (7) The ciphertext is decrypted with the random key, and (8) the plaintext is hashed into a temporary digital fingerprint to compare and validate the fingerprint immutability (Binder, 2002; Vacca, 2004).

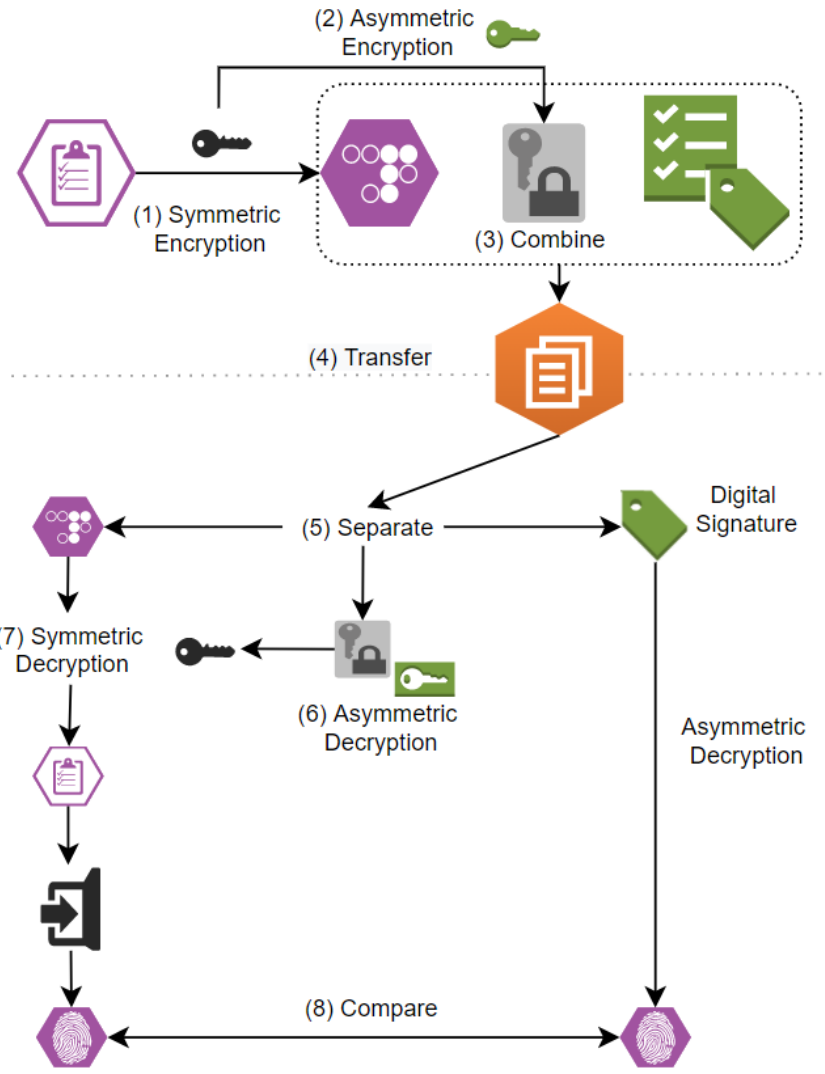


Figure 29 Digital signature associated with message encryption inspired by (Binder, 2002)

4.4 Stakeholders

According to the ISO, a stakeholder is a "person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity" (ISO 73, 2009). For this thesis, stakeholders will be involved and could affect and/or contribute to the RMP. Therefore, it is crucial to identify these *involved actors* and their contribution to the process since the stakeholders' concerns typically focus on the actor's influence in decision-making. Although, there are other options to consider, such as (Rausand, 2011):

- People who are affected directly by a decision to take action on any issue or project
- People who are interested in a project or activity want to become involved in the process and seek an opportunity to provide input
- People who are more generally interested in the process and may seek information

- People who are affected by the outcome of a decision but are unaware of it or do not participate in the stakeholder process

The involved actors in the RMP could be similarly identified with the following considerations:

- People who are involved in the process and are interested in the adequate results of the project or activity. (By action)
- People who could affect the outcome and decisions of the process. They may have some kind of interest or role as an authority, but they do not participate in the RMP. (By interest)
- People who contribute with their opinion, knowledge and provide information to solve a task. (By task/contribution)

Thus, these could be divided into three major categories – Internal players, related players, and external players – which could be from inside the system as well as from outside it.

Internal Players (by action)	Related Players (by interest)	External Players (by task)
- Member of the Organization: Internal employees and authorities at any level - Risk Manager: Risk Assessor, Risk Communicator	- Regulators at any level - Environmental partners - Community and general public - Authorities at different levels - Contractors and suppliers - Shareholders - Investors and creditors - Education organization - NGO's - Communication and media groups - Infrastructure/Energy groups - Employees	- Technical - Organizational - Communication and social media - Strategy (business) - Management and compliance - Operations and sales - Financial and Legal advisory - HR - Technology/IT - Health and Safety - Environmental and sustainability

Table 3 Involved actors at RMP

1. **Internal players** are those that are involved directly in the process, have the knowledge and skills that would contribute – do an *action* – in the RMP. An action would be considered as any analysis, assessment, communication, or decision that is required within and along the process. These people could be the RM, and members of the organization – internal employees and authorities at any level, as presented in Table 3, and their relevance is explained in Table 4.
2. **Related players** are those that have any kind of *interest* in the system but do not have a specific task at the RMP. Likewise, they could have authority and/or regulatory roles. Table 3 presents an idea of the group of people that could enter this category – but not limited to – which could also include shareholders and employees, and their relevance is explained in Table 4.
3. **External players** are those that can provide information or represent the view or interest of the given project, they are related to the process but do not participate in the analysis. Thus,

are considered as actors that do a specific *task* in the RMP. Also, they could be called *external risk assessors* (ERA) because could be risk owners that provide information related to risk identification. Table 3 present a group that could be considered – but will not be limited – as external players, and their relevance is explained in Table 4.

Players	Relevance
Employees – RMP related	Considered as an internal player when they are involved in the risk identification and/or risk monitoring, or by participating in expert elicitation. Considered as a related player when they only have an interest in the outcomes and implementation of measures.
Authority	Considered as an internal player when is involved within the RMP. Considered as a related player when they only provide regulations according to the organization.
Risk Manager, Assessor, Communicator	Considered as an internal player, they are entirely focused on the RMP.
ERA – RMP related	Considered as external players, they could be the people that could provide existing data, that will eventually be used to do the risk estimation. Also, could communicate strategically the outcomes.
Regulator	Considered as a related player and laws provider. Through the laws, they can monitor any related implementation.
Environmental, Infrastructure/ Energy groups	Considered as related players, they could be advisors and provide specific awareness.
Community & general public	Considered as related players, they could have an interest in the outcomes or the process. Also, they could show opposition to the project, measures or anything related.
Contractors & suppliers	Considered as related players when they only have an interest in the outcomes and implementation of measures.
Shareholders, Investors & creditors	Considered as a related player, they only have an interest in the outcomes. They need to be kept satisfied.
NGO's	Considered as related players, they could have an interest in the outcomes or the process. Also, they could show opposition to the project, measures or anything related. They need to be kept satisfied.
Communication & media	Considered as related players, they could have an interest in the outcomes or the process. Also, they could show opposition to the project, measures or anything related. They need to be kept satisfied.
Employees – RMP Non - related	Considered as related players, they could have an interest in the outcomes or the process
ERA – RMP Non-related	Considered as external players, they could be advisors that about financial, technological, strategies and any other kind of support.

Table 4 Players and their relevance in RMP

Since the involved actors also have different attributes, a stakeholder analysis is required to identify which of them are key players in the RMP. Initially, the stakeholders could be divided into two major categories – *internal stakeholders* and *external stakeholders*. The internal stakeholders are all those directly related to the RMP within an organization; as explained before, this includes the internal players, decision-makers, and shareholders (if any) and ERA from departments within the organisation. The external stakeholders are all the others who influence from outside the company, which impact the projects but are not directly connected to the project. In this case, it could be the related players as well as external players depending on the project-specific.

The stakeholders that could influence a project will be presented next. This is done to understand the closeness, interest, and power of the participants in the RMP. In the case, four groups of stakeholders have been identified – company, consultants, regulators, and co-operators – each of them with specific involvement in the RMP.

Company

The chosen company for this project has a simple organizational structure. In other words, the company structure has low complexity, the order of management will be mutually agreed, and the coordination and supervision will be direct. There could be an organizational chart with a focus on leaders without the need for formalities. (Ahmady et al., 2016) The company is formed as presented in the organisational chart in Figure 30. Hierarchically, the company has a board of directors, a board of managers, and the employees of each department manager that exist in the company, these will be used for the stakeholder analysis.

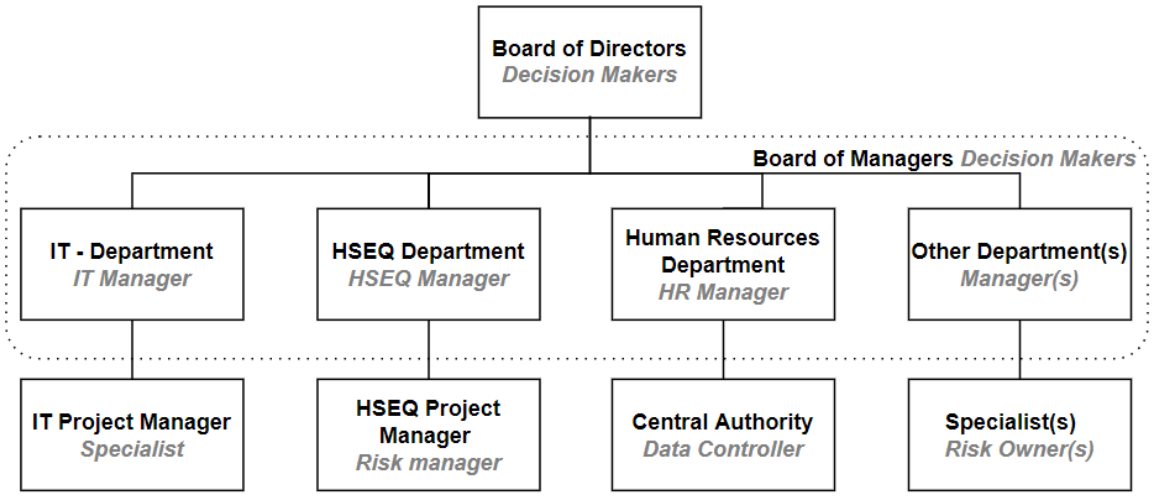


Figure 30 Stakeholder power-interest categorization

Board of Directors

The board of directors is formed by executive directors, shareholders representatives, and outside independent directors. The chairman board and the CEO will represent this. The role of the board is to estimate the evolution of the socio-political environment and reduce the

complexity and uncertainty involved; thus they must monitor the results (Van den Berghe & Levrau, 2004). In addition, "boards must establish proper rules in order to prevent mismanagement and monitor these rules. Installing a system that discourages corruption is a minimum condition" (Van den Berghe & Levrau, 2004). Likewise, the board is normally considered for a company's decision-making group.

Board of Management

The board of management is formed by the managers of each existing department within the company. Its chairman is the CEO of the company to whom managers report progress and needs of their department in representation. The managers that are part of the board are from the IT-, HSEQ-, Human Resources- (HR) departments, and other departments could report to a specific risk-related task, as required for the RMP.

Employees

The employees are those who belong to a specific department that is involved in the process:

- **IT project manager:** belongs to the IT department and is the specialist owner of the interface between the new technology and the existing systems in the company. In the RMP, he/she could participate as a collaborator or ERA for the risk identification of the interface
- **HSQE risk manager**: belongs to the HSQE department and is considered as the risk manager in charge of the RPM. This manager could act – at the same time – as the risk assessor and the risk communicator, or these positions could be taken by more than one employee that belongs to the same or other departments, like communication
- **Central authority – data controller:** (GDPR specialist) belongs to the HR department who is in charge of collecting the employee information, including sensitive information that must be kept by following the General Data Protection Regulation (GDPR). According to the GDPR, there must exist a *data* controller who is a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". (European Union, 2016) Among his/her responsibilities are to apply the appropriate technical and organizational measures to be able to demonstrate and guarantee that the processing is carried out following the regulation and to apply adequate data protection policies (European Union, 2016)
- **Specialists:** also called ERA, can be any other company employee who has the responsibility of reporting existing risks in their department. They could also be intermediaries between activities that require external collaboration, so they could be transmitters of external risks

Consultants:

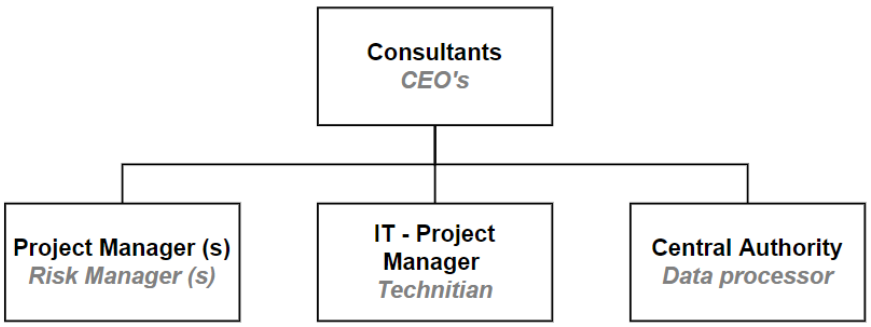


Figure 31 Consultant Organizational Chart

The consultant's company could be a small and independent consultancy that provides a new technology for the RMP. It has a simple structure where the owners (CEO's) are also the employees/specialists. Therefore, the decisions taken will be for mutual agreement between the owners.

Project Manager – Risk Manager

The project managers are the owners of the project and will do the complete RMP and provide the new technology. Therefore, they are considered RM's that will assess and communicate the risk. In addition, they will be the ones who have contact with the majority of the actors involved to provide traceable and secure risk management.

IT- Project Manager

The It-Manager is the physical creator of the technology for the protocol behind the blockchain. This person is responsible for creating, building, and implementing the technology. Among his/her responsibilities are the direct dialogue and connection with the company's IT specialist, throughout the implementation and interface with the company.

Central Authority – data processor

As well as in the company and according to the GDPR, there is a need for a *data processor* who is a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (European Union, 2016). He/she will carry out the data processing on behalf of the controller, with processors that offer sufficient guarantees to implement the appropriate technical and organizational measures. Furthermore, he/she must inform the controller if another processor is required and process the authorizations according to the regulation. Therefore, there must be a contract or other legal act that binds the data processor and the data controller at the company. This contract must also establish the object, duration, nature, the purpose of the treatment, the type of personal data, the categories of interested parties, and the obligations and rights of the controller. (European Union, 2016)

Regulators

Danish Government

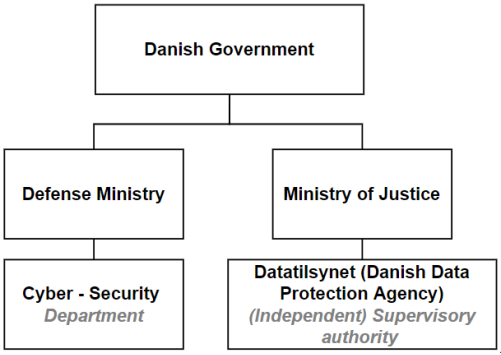


Figure 32 Danish government IT/Data structure

The Danish government is the executive power in Denmark; it is a right that has been given to them by the constitution. Their role is to make sure that the rules and regulations that are agreed on in the Danish parliament are being followed and work in the Danes best interest. Hence, they can make new laws- and regulations proposals that can improve Danish population wellbeing (Folketinget, 2016). Two ministries are working on IT and data protection – the Defense Ministry and the Ministry of Justice. These ministries have some regulations that are needed to be followed to be able to use the system.

- **The Ministry of Defense** is managing the Cyber-security centre, which has the purpose of protecting Danish citizens and companies against hacker attacks and cyber threats. They have an interest in increasing safety by utilizing new technologies (Forsvarsminiseriet, 2020)
- **The Ministry of Justice** has made the Danish Data Protection Agency, which ensures that private data is protected. It can guide the public and originations regarding how to handle people's private data. If someone does not follow the regulations, they conduct an investigation. They are in close collaborations with other authorities in the EU and ensure that the data controllers and the data processor are well educated in the art of data protection (Datatilsynet, 2021)

European commission

The European Commission (EC) is a regulatory body when it comes to the protection of natural persons with regard to the "processing of personal data and the free circulation of such data" (European Commission, 2018). Therefore, it has generated a regulation that seeks to strengthen the fundamental rights of people in the digital age and facilitate business by clarifying the rules for companies and public bodies in the digital single market. This regulation has been applied since May 25, 2018 (European Commission, 2018).

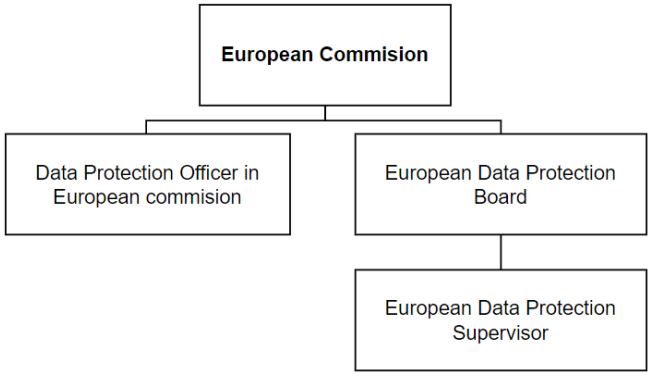


Figure 33 European Commission structure

- **European Data Protection Board:** (EDPB) is an independent European body composed of representatives of the EU countries and the European Data Protection Supervisor. The board ensures the application of data protection regulations in the EU and is established by the GDPR (European Commission, 2018)
- **European Data Protection Supervisor:** (EDPS) is an independent body of the EU established by the GDPR. It is responsible for monitoring that the European institutions apply data protection regulations and for investigating complaints (European Commission, 2018)
- **Data Protection Officer in the European Commission:** is appointed by the European Commission and is responsible for the monitoring and the application of the data protection regulations in the European Commission. The officer independently guarantees the internal application of the rules and cooperates with the EDPS (European Commission, 2018)

Co-operators

Co-operators could be anyone that the company needs to communicate with, like suppliers. They are interested in exchanging information safely but do not have any involvement in the implementation of the ledger and the RMP.

Although, this categorization does not allow the correct identification of stakeholder participation in the process. Since not all stakeholders are equal, nor do they have a saying or control, it is relevant to identify the stakeholders who actively participate in the RMP. By identifying the people who will handle the necessary information in the process, the development of a generic architecture for the RMP will be more precise. Similarly, active stakeholders within the architecture will be granted the necessary access, which will provide security when complying with the traceability requirement. Therefore, it is necessary to analyse the attributes that the stakeholders have. A power and interest matrix analysis could help with the prioritization of the stakeholders when the two attributes are mapped.

4.4.1 Power – Interest Matrix Analysis

This is a two-dimensional analysis that compares the attributes of power and interest of the stakeholder concerning a specific project, for this thesis, the stakeholders at a generic RMP. Therefore, power will be considered as the "strength or influence in a particular area" (Oxford University, 2021) of the RMP. As for the interest, it will be "a connection with something that affects your attitude to it, especially because you may benefit from it in some way" (Oxford University, 2021a). These will be the considerations to analyse the involved actors in the present generic RMP and categorize them into stakeholders.

Stakeholder			Relevance	Power	Interest
INTERNAL	**Company**	***Board of Directors***	Considered as related players. Decision-makers, provide objectives	High	Middle
		Board of Managers	Considered as external players. Share information from RM to the board of the directors, could take some decision in advance stages	Middle	High
		IT Project Manager	Considered as an internal player. In charge of the interface between companies	Middle	High
		HSEQ Project Manager	Considered as an internal player. RM of the project	High	High
		ERA: Risk owners	Considered as external players. Help with expert elicitation and data for risk identification for risk estimation	Low	Middle
	Consultants	***Risk Manager(s)***	Considered as internal players. RM of the project	High	High
		IT Project Manager	Considered as a related player. Creator of the new technology and in charge of the interface	Middle	High
EXTERNAL	**Legislators**	***Danish Government***	Considered as related players. Rule provider – regulators	High	Low
		European Commission	Considered as related players. Rule provider – regulators	High	Low
	Co-operators	***Suppliers***	Considered as related players. Share Information and help for risk identification	Low	Low
	Company	***ERA: Data Controller***	Considered as external players. Regulator	Middle	High
	Consultants	***ERA: Data Processor***	Considered as related players. Regulator	Middle	High

Table 5 Stakeholders power – interest categorization

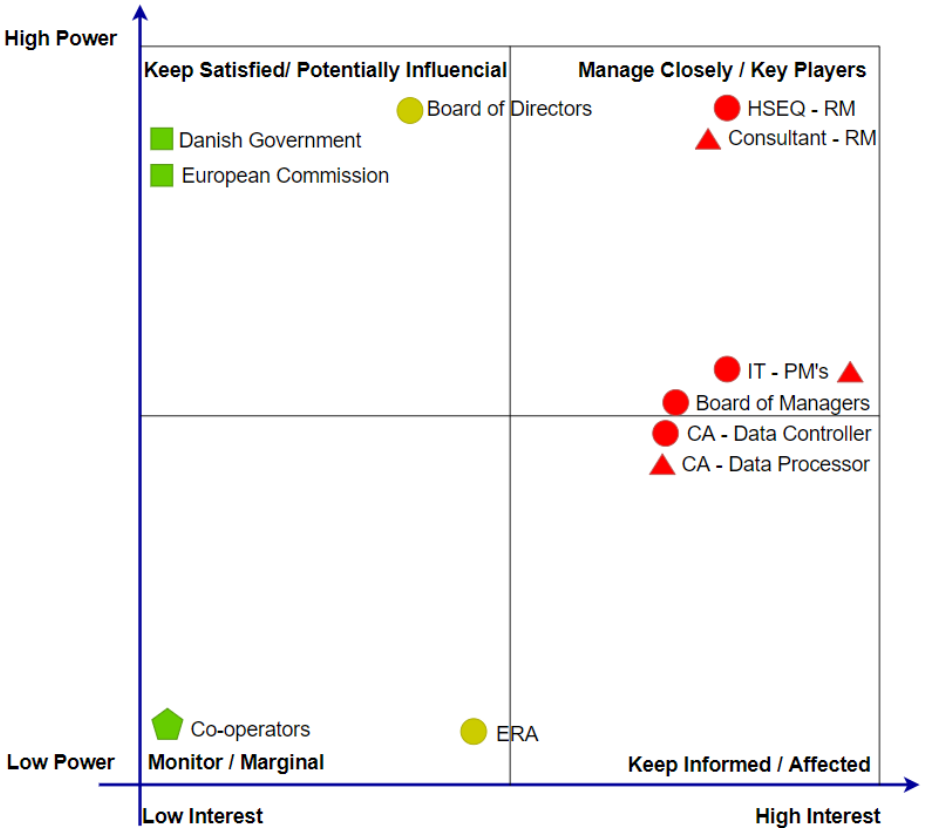


Figure 34 Power – Interest Matrix, Generic Risk Management Process

The identified key players are the RM's from the company and the consultants; the influential stakeholders are the legislator group – the Danish government and EC – and the board of directors. In the lower level with no power and no interest are the co-operators. However, this analysis still does not reflect the real involvement of the stakeholder in the RMP, only how influential they could be in the process.

Even though, the power and interest of each stakeholder give the relevance of why to consider each of them in risk management and how to treat them. The main purpose of the analysis is to identify who has a saying and who is directly involved in the RMP, and this 2-D analysis does not help to the right identification. To get a better view, a 3-D analysis is proposed next, where it will consider one more attribute – level of *involvement*.

The reason why this involvement is considered is that some "minimal or usual" tasks in the process could cause an error that leads the system to collapse, especially when the process relies on technology. A recent example of how an error in other departments could affect a process is the Facebook global outage, where a routine maintenance error occurred in their network centres. An attempt to assess the capacity of the global backbone, ended up inadvertently cutting off all connections with Facebook's data centres globally (The Guardian, 2021). "The failure of such key internet players had a knock-on effect on individuals and businesses across the globe" (Wakefield, 2021). Approximately 10.6 million problems were reported worldwide, a possible loss of revenue for Facebook of almost $ 60 million and the shares dropping by nearly

5% (Wakefield, 2021). Consequently, the key players at the RMP and their functions in the process must be identified, their tasks, and their involvement, which will provide a better identification of the potential risks.

4.4.2 Nautic Analysis: Power – interest – proximity

The Nautic analysis considers three attributes and was inspired by the *stakeholder's map PM Nautic.* This method is a "system of radial sectors, which can represent generic groups of stakeholders" (Cenek & Částek, 2016) with its attributes with a variety of representations such as colour, shape, and distance. The chosen attributes for the case analysis were power, interest, and proximity since these attributes could help determine the real closeness of the actors in the project. Therefore, each radial sector will present the proximity of the stakeholders to the RMP. Involvement will be considered as "the act of giving a lot of time and attention" (Oxford University, 2021b) to actions directly related to RMP. Hence, the closer a stakeholder is to the centre, the higher involvement they have.

Figure 35 presents the forms of representation of the involved actors and their attributes. To represent the actors, shapes are chosen; the change of the shape size will show the power; the interest will be presented in the traffic light colours, and finally, each radial sector will be highlighted with a darker colour to show the proximity in the graphic.

Figure 36 presents the Nautic Analysis where the internal and external stakeholders are categorized according to the attributes. From the mapping, it is visible that regardless of the power or the interest levels, the involvement in the RMP is reduced to specific stakeholders. There, it is highly noticeable how the external stakeholders have no direct involvement with the process, their common interest could be the outcomes of the process and the decisions taken after it. The non-involved stakeholders are the legislators, board of directors, board of managers and data controller. They could be managers in general concerning how the outcomes of the RMP could affect their department measures. Also, there are authorities that have a saying in the process; they could give approvals, reporting or monitoring.

Those stakeholders that might be related to the process are the ERA and Co-operators, which could help with the risk estimation and monitoring. Meanwhile, as expected, the highly involved actors are the RM's and the IT-PM's from both the company and the consultants and the data processor. The highly-involved actors are employees working in the RMP and the RM in charge of the project, that do most of the risk management, risk assessment, and risk communication. The IT-PM is more involved in the process because a mistake related to their involvement could compromise the whole process, since this architecture and functionality is completely dependent on the technology, as previously explained in the Facebook outage example.

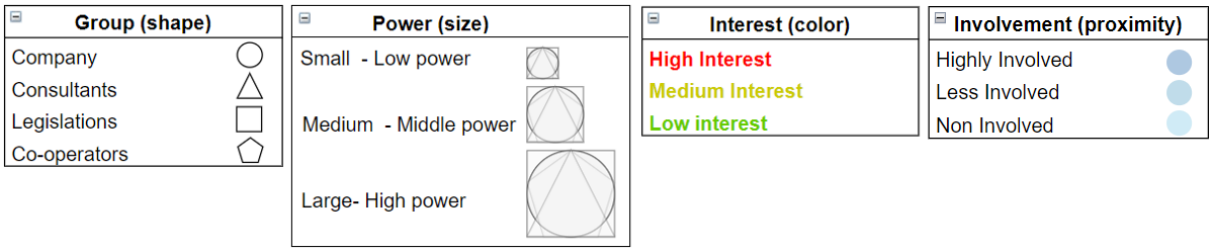


Figure 35 Attributes for Nautic Analysis, Generic Risk Management Process

Figure 36 Nautic Analysis, Generic Risk Management Process

5 Architecture

In the following section, the architecture proposal for an RMP based on blockchain technology that includes PKI will be covered. Furthermore, to decide the correct PKI method to adapt to the system, it is first necessary to determine the characteristics that are required for this proposal. Therefore, the aim is to include at least two fundamental characteristics in the system – authenticity and integrity. PKI not only provides the two desirable characteristics but also includes non-repudiation. Consequently, this section explains the features chosen to be adapted for the blockchain protocol and PKI that will help the validation of the participants throughout the RMP.

5.1 Central Authority

For the architecture, there will be two CAs, an external server (consultant) and another internal belonging to the company, which could also function as RA. These two CAs will be validated with cross-certification, from there could be leverage to the web of trust that will allow the exchange of keys.

The external CA will be the one who has the repository, hence the issuance of the keys and their certificates for the blockchain users. When the validation of the keys – used to sign the documents – is required, it will be authenticated through the certification validation path. This process is illustrated in Figure 37.

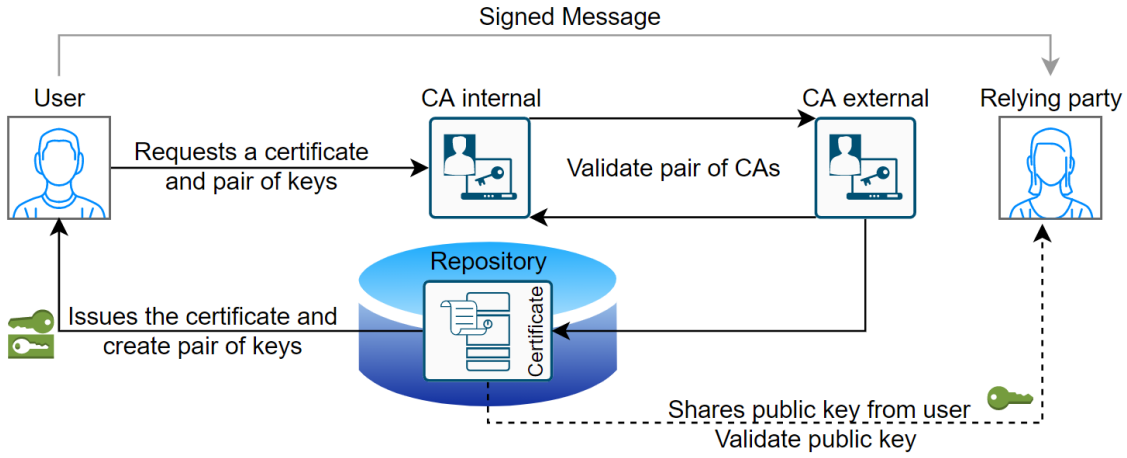


Figure 37 Certificate process and key assignation

5.2 Keys

To access the RMP's blockchain, it is necessary to create a pair of keys – public and private. For this the keys will be assigned in the following way:

- A pair of keys – will be assigned to a person when they are been certified and created as users. The public key will be the address from and to where the documents will be sent
- The RMP will be assigned with a key pair, the-public key will be shared with all users while the private key will be stored by the CAs. The private key will only be used by the CAs when a relying party requests the validation of some user
- The keys will be valid as long as the user is part of the team or the company and may require renovation whenever any basic information has changed such as address. The unsubscribe keys will be stored in CRLs for future authentication
- The private key will be automatically linked to a wallet. Also, it will be able to generate more public keys for other projects
- All the public keys will be certified automatically by the CAs that will issue a new certificate of authenticity for each key created
- The public keys will be automatically linked to the user's work

5.3 Wallet

Once the user has been certified and has the key pairs, a wallet will be created on the server. This wallet will:

- Allow the user's pair key storage
- Allow the generation of public keys
- Interaction with the CAs server to authenticate the new public keys
- Storage of certificates belonging to the public keys
- Interaction with the network – account state

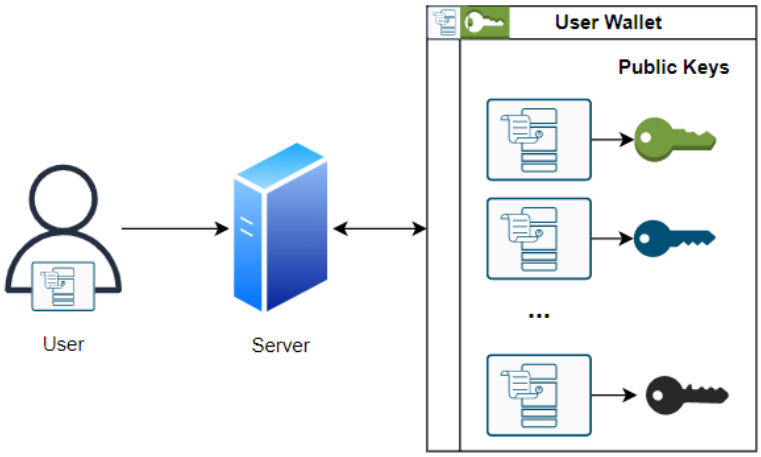


Figure 38 Wallet interaction

5.4 Access

To access the blockchain, the user needs to be registered in the system, and the only way to do that is by contacting the external CA. Upon entering the system, the user must choose the

organization to which he/she belongs, type its username, and enter with the public key corresponding to the process.

PKI will authenticate the used key virtually, which means that the CA will validate if the public key has a granted certificate. Once the key has been validated, then the user will enter the network.

5.5 Network

The network type that the RMP system will run on is the consortium network. The reason is that the external CA controls the access at the request of the companies. When the users have been given access, they are allowed to contribute to the blockchain. However, limited access could be implemented so the users can only see specific parts of the blockchain. The company could choose to do this if they are not interested in sharing the whole chain or make it easier for the contributors to select the right tool by eliminating the irrelevant choices.

The ability to choose who has access to specific parts belongs to the company, while the access to the server – hence the blockchain(s) – and the functionality is kept at the consultant company. The reason for the division is that it will create a faster change if a user needs to have more accessibility. Then an admin/controller at the internal CA can change it without talking to the consultants first.

5.6 Blockchain design

This section will give the blockchain design for RMP, what protocol will be required, what the block will consider and how it will look like.

5.6.1 Protocol

For the ledger, the protocol is based on the Ethereum enterprise protocol since it allows the usage of smart contracts, making the ledger more adaptable to different companies' needs. For example, if a company requires a specific tool for risk management, a new risk tool can be developed and implemented without creating a new blockchain. This will allow to maintain the work on the existing chain.

Consensus mechanism

The proposed consensus mechanism in the ledger will be called *Proof-of-Ownership* and it is built on the combination of PoS and PoW. Everyone can validate their block and upload them to the blockchain, making the users their own validator. When the block is uploaded, their digital signature will be generated in their work, and it will automatically sign the block – and everyone who has contributed to it. This will allow them to protect their work and help track specific users and preventing others from claiming the right to that work.

5.6.2 Block

The block will consider all the characteristics necessary for the RMP; therefore, the following will explain the changes and adaptations required:

Account state

The account status is used to store the user's credentials – part of the wallet information. This will automatically create a link between the information and the creator – user. The account state will have the same configuration as in the traditional account state, only with the changes in the balance function as presented in Figure 39, and consider the following:

- The account statement acquires and indicates the public key
- This will contribute to linking the information to the stateRoot in a block. Therefore, the information will be automatically linked with stateRoot which will be linked with their public key

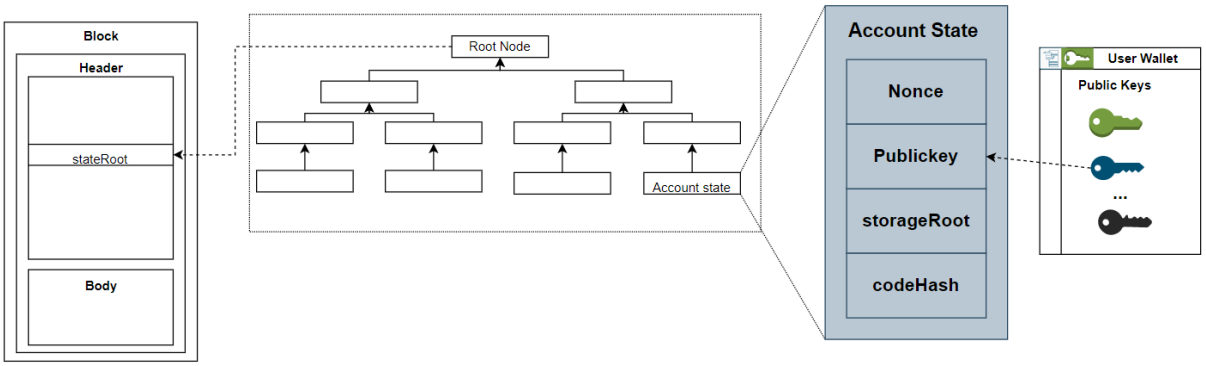


Figure 39 Relation between the account state and the block

Transaction

The transaction is reduced in the number of requirements needed. The gas function is being removed since the system is privately controlled and does not need rewards to select the transactions by the miners. The final transaction model is presented in Figure 40 and considered the following:

- The value part is the data sent to the server and is chosen based on the template required in the RMP. The template is predetermined – based on the function that is required
- The address is changed so a user can only send the block to the blockchains they have access to
- The signature will be the digital signature of the shared information

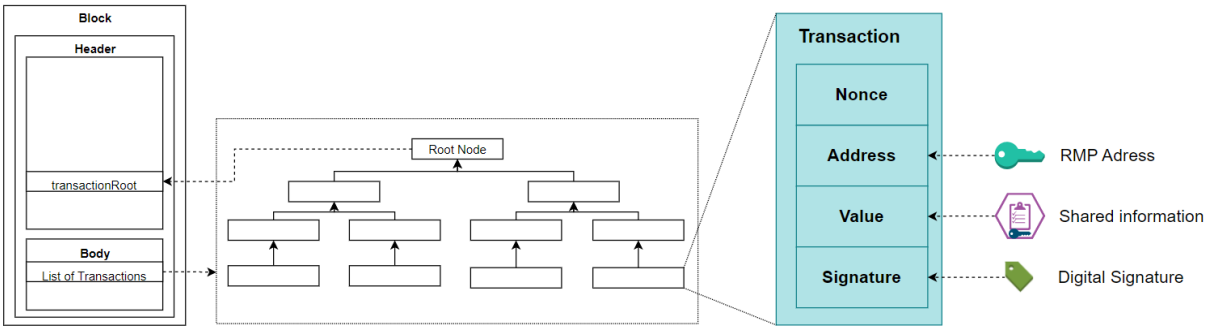


Figure 40 Relation between the transaction and the block

Blockheader

The blockheader will not consider three of the standard criteria – gasLimit, gasUsed, beneficiary. The block will operate in two layers, the front page and a bottom layer – data page – both can be accessed when a block has been uploaded to the blockchain. The reason to do it is that when a user has to contribute with data, it needs to be as smooth as possible, easy overview, and not confusing. Therefore, the front page will be the interactive layer, while the data page will be the network-related layer. By removing the technical aspects to the bottom layer, the intention is to give users – with not strong IT technical knowledge – the ability to add or read information more easily.

The front page is presented in Figure 41 and will:

- Specify the block number
- Provides easy interaction with uploaded information
- Present the organization ID and the names of the members of each organization, that have contributed to the work
- The ID will be automatically generated since is the digital signature of the information.
- Present the possibility to upload and create a smart contract
- Present the possibility to upload extra data that must contain the public key and be digitally signed

The data page will:

- Contain the validation data for that specific block – parentHash, block number, mixHash, ommerHash, timestamp, nonce, difficulty, logBloom, stateRoot, reciptRoot and transactionRoot
- Contain the validation data of the shared information which is linked with the public key
- Contain the validation data of the user that has created the information which is the digital signature

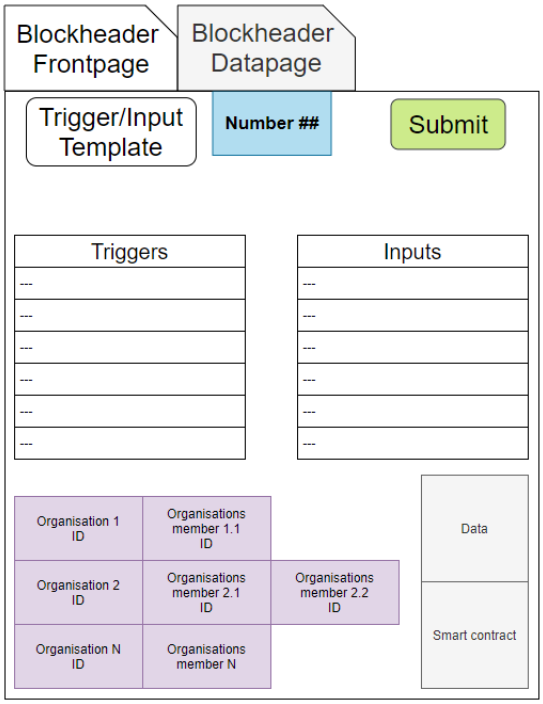


Figure 41 Blockheader front page, Trigger/Inputs Template

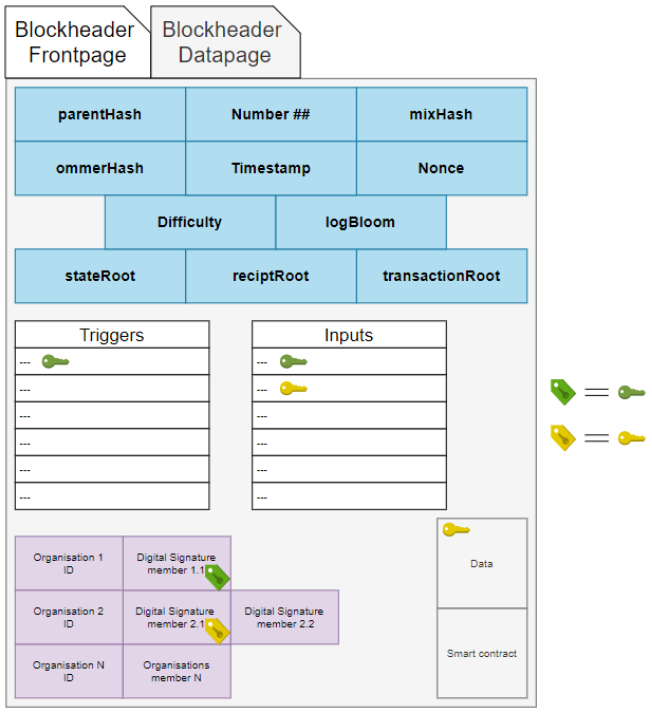


Figure 42 Blockheader data page

Templates

The RMP in the block is based on templates to ensure that the RMP is done in the correct order. The templates would be constructed from the brainstorming lists to a more complex calculations setup, like the templates presented in Figure 41 and Figure 43. However, these can only provide

setups and are still relying on the information the users put in. If a template does not exist, it would be possible for the users to create a specific template, but it needs to be suited to a specific category of the RMP. Thus, the system will know in which stage to allocate it.

The templates features will contemplate the following:

- The information inside the template will be related automatically with the public key – stateRoot
- After the template has been filled in, the digital signature will be generated from the information

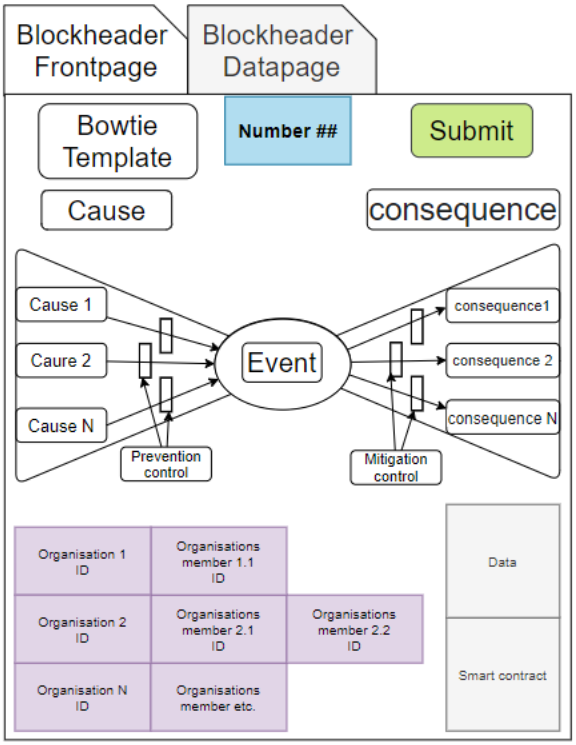


Figure 43 Templates example Bowtie inspired by (ISO 31010, 2009)

Several useful tools can be used at different stages of the process. Therefore, to determine which will be the most suitable templates to be used, the RM will have to analyse what the project needs are. Also, the RM will be able to adapt the tools at the beginning and during the process, either from the existing or the creation of new ones.

5.7 Systems Interaction

An RMP will start when there is an identified potential risk that has been proposed and taken into consideration by an RM. The RM will be the person leading and working at the process at all stages; consequently, he/she will be the one that will initiate the blockchain by creating the genesis block.

Therefore, the genesis block could be considered as the "instruction" block because it is where all the guidelines will be set. This needs to be according to the need of the project and could contain the following, but not limited to:

- List of stakeholders that will collaborate, stating the organization they belong to and its organization ID
- Share the public keys of all the stakeholders
- Any kind of instructions
- Templates that will be used and in which stages

The following block should be the objectives and preferences considered important for the project to make the best decision. This means that the decision-makers should be the creators of this block.

Once the users have access to the blockchain network, they will be connected to the server first, as presented in Figure 44. When the connection has been established, a screen will present the options to choose on which project they will want to contribute. The projects will be predetermined by the controller on the ledger.

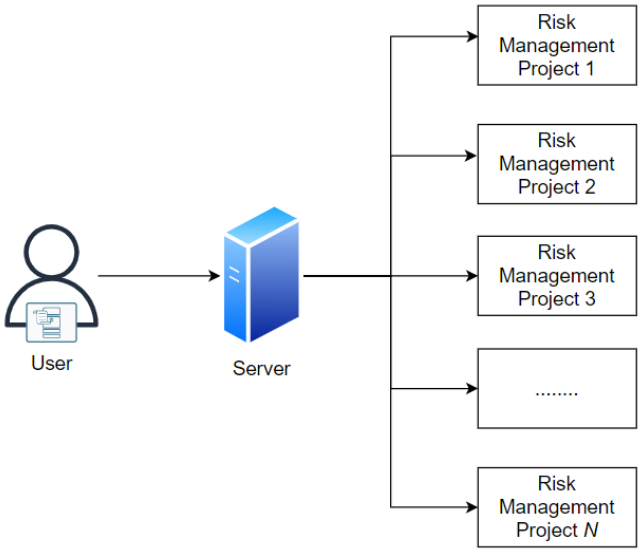


Figure 44 Access to the RM project

Next, the stage in the RMP can be chosen. The reason for selecting the stage is to ease the selection of the templates that are associated with it, as well as, to choose the specific tools available. Figure *45* presents how a user can choose a stage to contribute to. However, if the previous stage is not completed the next one will remain inactive, until it detects that the previous stage has been completed.

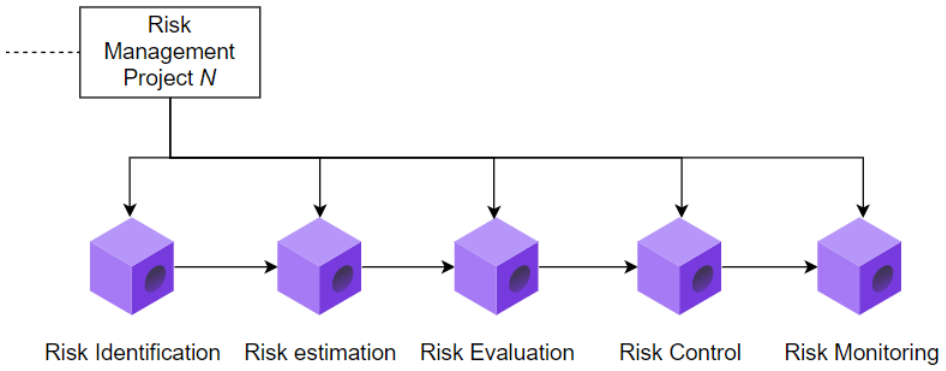


Figure 45 Selection Phase

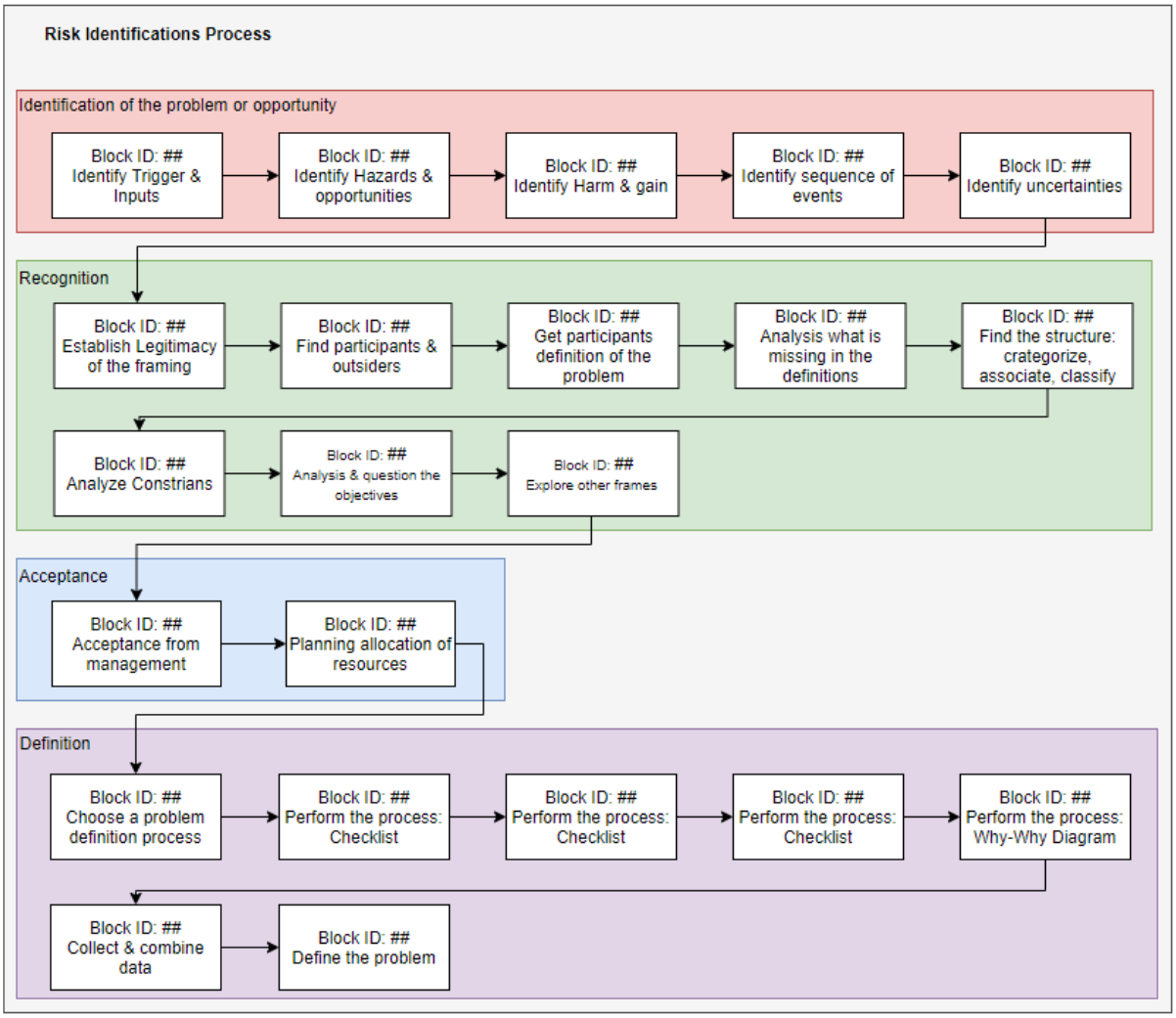


Figure 46 Blocks connectivity example

When the stage is selected, users will have access to the interface, which will allow them to select the part in which they can contribute. This means that all the templates that could be used for the chosen stage will be displayed. The documents will work in a hierarchical system, which

indicates that they will need to be connected to the right template to be uploaded. Figure 46 present an example of the tasks that are needed to "complete" the risk identification part.

After choosing the template, users will interact with the block's front page, while the data page will obtain the required information from the user. When the user has contributed the information, the next step is to click on submit, which will activate the upload function. At the same time, this will generate the digital signature that will be stamped on the data layer and later the block will join the blockchain.

As mentioned, when the user is interacting by filling in the assigned document, it will automatically reflect the user's public key on the data page, as presented in Figure 42. In addition, once they have sent the information, the digital signature will be generated automatically as follows:

1. The fingerprint will be generated considering the document and the public key – included in the document

2. The fingerprint and information will be encrypted asymmetrically with the RMP public key

3. The signature will be stamped on the block's data page

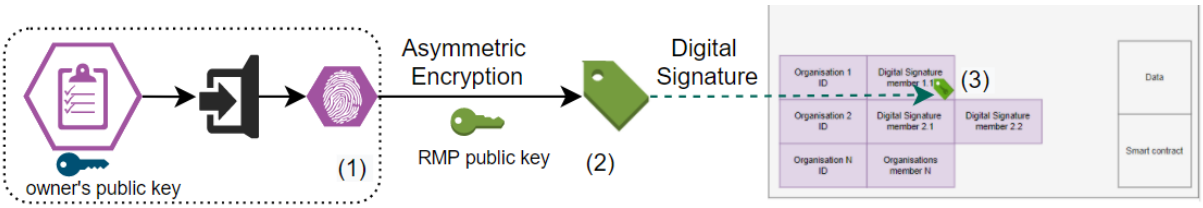


Figure 47 Digital signature stamped process

On the front page, the organization's identification and the user's name will be presented so that everyone can see whom the contributors are, as presented in Figure 48. Everyone with access to the blockchain will be able to see this information. However, not everyone will be able to authenticate the digital signature, the CA will do this upon request.

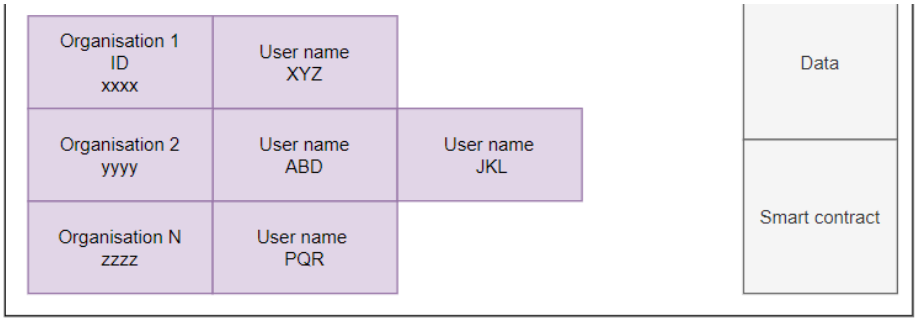


Figure 48 Bottom part of the Frontpage

Every time that a user is created and certified, the initial form will include the organization ID from where the user belongs to. This organization ID is created with the first user from that

organization, this will be tracked and stored by the external CA. From here, the public keys will be linked to the user and assigned the organization ID to be automatically linked at the block.

5.8 Authentication

Since blockchain is a system that promotes traceability and trust, where each transaction is visible to users. The RMP blockchain system seeks to maintain the same characteristics and in addition, the digital signature technology will be included to authenticate the identity of the users. The way that the PKI system is presented in Figure 49 and will work as explained next:

1. The documents that will be created in the block – by the users –, will contain the creator's public key. In this way, the information is linked with the creator, which will help with the identification of the owner
2. The combination of both will pass through hash computing to create the digital fingerprint of the document
3. The digital fingerprint will be asymmetrically encrypted with the public key created for the RMP to create the digital signature
4. The original document with the digital signature will be now uploaded to the block.

When someone needs to identify a document's owner, it will be required to contact the CAs to decrypt the signature. This will allow the fingerprints comparison; to compare the address from where it has been shared with the public key inside the document and certify the public key ownership. This process is the following

5. Separate the document and the digital signature and get the public key from the original document
6. Hash computing the original document to get the digital fingerprint
7. The CAs will decrypt the digital signature to get the digital fingerprint
8. Compare the digital fingerprint to prove the immutability of the document from the creation
9. The user will compare the documents owner's public key with the block address and ask the CAs validation
10. The CAs will authenticate and share the certificate of the public key ownership

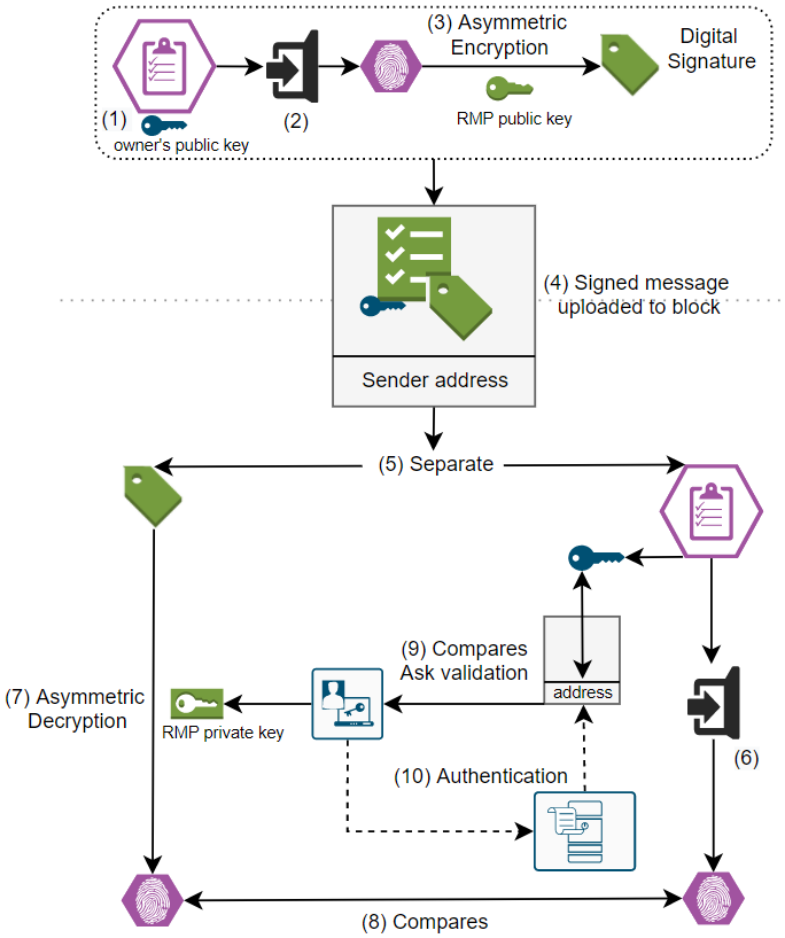


Figure 49 Authentication Process

6 Analysis

This section will cover inquiries that have been identified throughout the development of the RMP blockchain system. Therefore, it has been categorized into three sections – blockchain, users and safety.

6.1 Blockchain

6.1.1 How will the blockchain work?

The RMP blockchain is a combined system that will allow easy interaction with the user, and it will determine the proper order of the process. This blockchain will work directly in the block with the necessary templates for each stage and step, for which there are two layers, as presented in Figure 50.

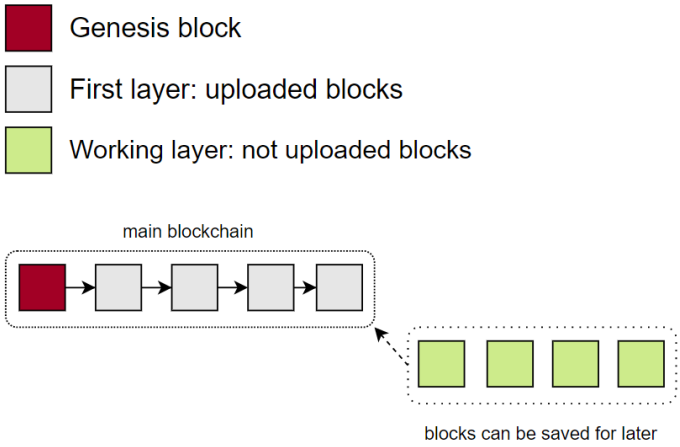


Figure 50 Blockchain layers

The primary layer is the blockchain that is uploaded and visual for everyone. Every block in this layer is finalized and contain all the characteristics (account state, transaction, and blockheader) and is connected in the chain.

The second layer will be the one that contains the work in progress. Here, one or more blocks will be presented in which the users are working. In this layer, the blocks will only contain the information linked with the users (public key), while the rest of the features will be created once they are uploaded. Also, these blocks could be able to be saved for later on the user's computer.

In order to add a block to the main layer, the system will recognize the order of the process. In other words, if a user tries to skip a step, the system will recognize it and prevent adding a block in a different order. The chained blocks will recognize the previous inputs, except for the first block in the risk identification stage.

What will happen with work in progress?

A regular blockchain does not save the work for later and requires that the information is completed and included in a single process. However, with the implementation of a second layer, the system will allow saving the work in progress.

The second layer can be saved in the user's computer and automatically eliminated once the block has been completed and included in the primary layer.

How would collaboration for one block work?

In addition to saving unfinished work, the second layer will allow collaboration in a block. By being visible the blocks and templates in which users are working, one user can decide whether to collaborate in a block or start a new one. This will represent that there is an agreement between the parties.

What if a template needs multiple user information?

If multiple user information is needed in one template, the second layer will allow this. Each input of each user will be automatically linked to their public keys. This will also represent that there is an agreement between the parties. Furthermore, when a stage reaches the step, in which it is necessary to create a report that collects the participation of more than one user, the information from the previous blocks can be used. This will allow not to lose the connectivity and agreement, and the new block will automatically recognize the existing public key in the information. By the automatic identification of the keys, the report block will seal it with the digital signature of the owner of the information used.

6.1.2 What if changes are needed in the blockchain?

When it comes to making changes or editing the information that is uploaded to the blockchain, there is a conflict between the RMP and blockchain concepts. The RMP is an ongoing process where the information can change as new knowledge is gained, or faults can need to be corrected due to the complexity of an RMP. Nevertheless, because of the immutability of the blockchain, it is not possible or at least not without consequences to make changes since it will disrupt the flow of the chain.

There are, however, some solutions that can make a redaction blockchain. All the redaction blockchain mechanisms have a function that can make changes/repairs the block and are based on four categories – Consensus-based, Chameleon hash, Meta-Transaction, and Pruning-based (D. Zhang et al., 2021).

Consensus-based is where an agreement is reached to make changes to the functionality of the chain. They provide security, consistency, and validity since the blockchain users have agreed to the system changes. However, these can be time-consuming to conduct and require a lot of storage space.

Chameleon hash is where a user can change the hashes on the network with a specific private key. They can create a trapdoor, that can change the information without creating a hard fork. The privilege of getting selected as a trapdoor keyholder is based on trust, as a result, an authority or a centralised user could be selected. This can make changes faster and do not increase the storage needed. However, it relies on specific users who can change the blocks' information without any permission other than they have been selected by others.

Meta-transactions focus on changing the information directly in the chain as well as on the local database. It uses a specific transaction function that allows editing to avoid large time usage and heavy cryptographic use. It suffers from key management and trust issues.

Pruning is developed to reduce the storage and computation power needed by deleting blocks that are not in use. The blocks to be deleted are selected by a system that looks at transactions that are independent of remaining or future transactions. Even though it reduces the storage and synchronising time, it comes at the cost of the protocol assuming which transactions are going to be independent, reducing the security by removing blocks.

For the proposed architecture

The proposed architecture has the function to change the information if needed after an agreement with the users. It is in the category of consensus-based method and will use the Practical Byzantine Fault Tolerance (PBFT). The PBFT consists of five steps – *request, share with users, Compare results 1, Compare results 2, and return* answer (S. Zhang & Lee, 2020), presented in Figure 51.

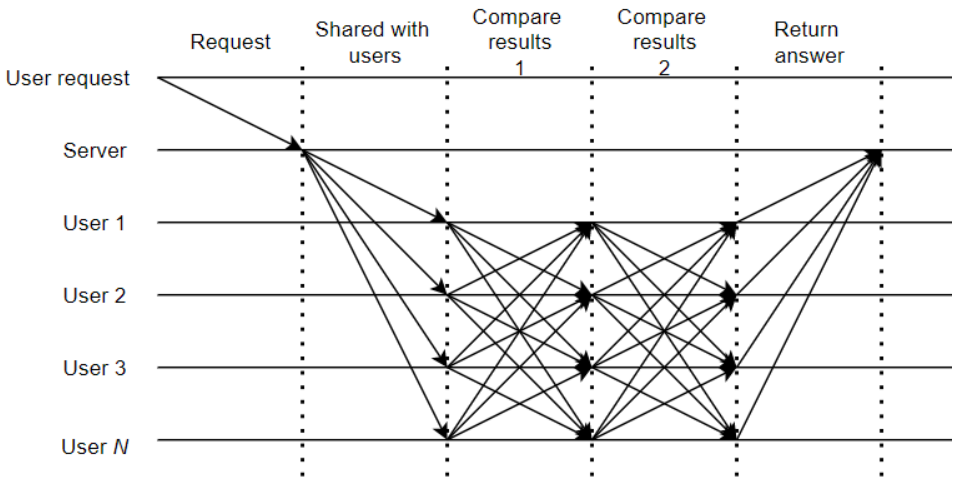


Figure 51 PBFT for changing, inspired by (S. Zhang & Lee, 2020)

In the *request*, a user requests a change by sending it to the server. From there, the server *shares* the requested information with every user in that step of the RMP. The user manually accepts or deny the changes. The mechanisms will *compare* the results with each other; this process is done twice. When the comparison has been completed, the *answer* is returned to the server, where the final consensus is calculated.

If there is an agreement to change the block, the chain will be copied, and the changes will be added to a new chain. This is possible because the templates are linked together in the input areas. The input areas will change to fit the changes and will mark the blocks in the chain where there would be a conflict. When all the changes have been corrected, the hashes will be calculated once again. The old chain will still be visible, but it will no longer be possible to add blocks to it, only for review. If the consensus is not reached the chain will stay the same, but it will upload a block that notices that a request has been made.

The advantages of this PBFT (Hooda, 2019; S. Zhang & Lee, 2020):

- All the users are communicating together to achieve an agreement
- The users will be known when they give their vote
- Low complexity compared to other consensus methods. Due to the low complexity of the mathematics algorithm, the power consumption is low
- Fast interaction after the votes have been given
- It gives a strong, consistent functionality and efficiency

The disadvantages of the PBFT (Hooda, 2019; S. Zhang & Lee, 2020):

- Scalability with the increased user. As more user is contributing to the RMP, there is a need for more time to get the results
- The Fault tolerance is 1/3 of the user, 33%. This means that a malicious user only needs to control 1/3 of the user result to stop changes from happening or create changes
- Storage increases for each change since the chain will be copied and added to the chain
- Uploading to the chain stops temporarily while the voting is committed

6.1.3 What will happen when there are ommerblocks?

The ommerblocks happened when two blocks were created simultaneously due to the time-specific upload interval. However, due to the instantaneous uploading feature being implemented into the architecture, the probability of multiple blocks being submitted simultaneously is reduced compared to uploading with a specific interval. The probability can be explained:

$$P = \frac{N * SB}{t}$$

Where

- N is the number of participants
- SB submitted block at the same time, $2 \leq SB \leq N$
- t is the time in seconds of a workday

The blocks will be uploaded in a hierarchy order. The order of upload will be possible to identify from the used templates since they will be given a value according to the stage and step. If two blocks are submitted simultaneously, a cue order will be applied and the upload will depend on

the value for the template. The ommerHash will function as a reference hash if there is a change, the hash will direct back to the last mixHash from that branch.

6.1.4 What if there is confidential information?

When confidential information – e.g. economic status – is required from specific stakeholders like external organizations to be shared the information, the stakeholder will have to upload the data encrypted to the block.

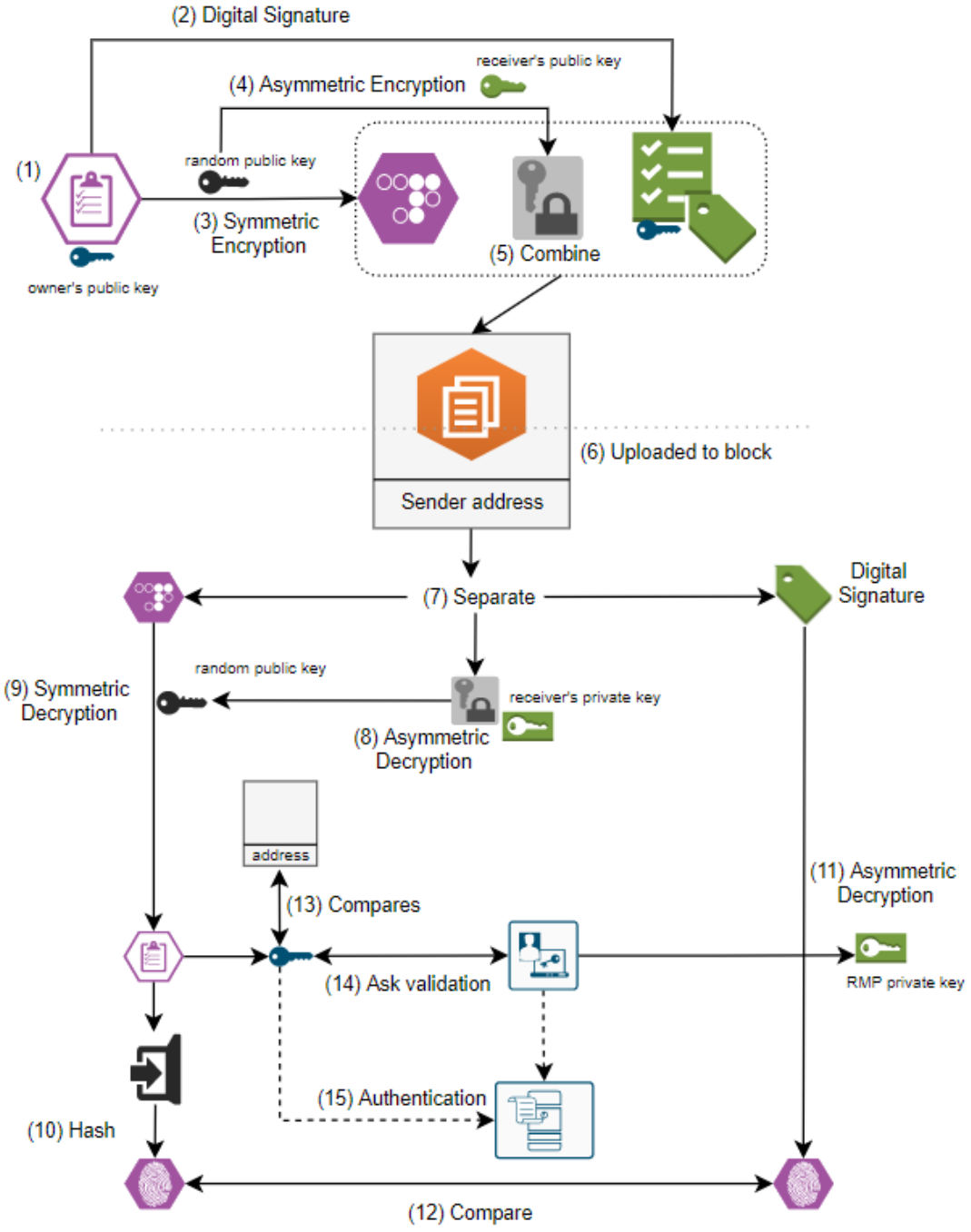


Figure 52 Encryption of confidential information and validation process

The encryption, decryption of the data, and the validation of the public keys are presented in Figure 52. To send the information confidentially, the sender must:

1. Include his/hers public key in the information
2. Create the digital signature
3. Symmetrically encrypt the information with a secret random key
4. Asymmetrically encrypt the random key with the receiver's public key
5. Combine the encrypted information, the digital signature, and the encrypted key
6. Upload to the block

To decrypt the message the receiver must:

7. Separate the encrypted information, the digital signature and the encrypted key
8. Asymmetrically decrypt the random key with the private key (receivers)
9. Symmetrically decrypt the information with the random key

To check the integrity of the information and validate the owner of the information it is necessary to:

10. The information has to be hashed into a temporary digital fingerprint
11. Contact the CA to asymmetrically decrypt the digital signature with the RMP private key
12. By comparing the digital fingerprints, the information is authenticated as the original. This means that the information was not modified during the transfer
13. Also, it is necessary to compare the public key from the information with the address from the block
14. If the comparison is a match, then it is necessary to ask for the public key validation
15. The CA will certificate the public key and authenticate the owner

6.2 Users

6.2.1 What if a user leaves?

When certifying public keys, temporality can be incorporated. This can be done considering two aspects

1. The levels of interest and the type of participation of the user

2. If the user belongs to external organizations

As observed in the stakeholder analysis, it was determined that 5 out of 12 stakeholders are considered external stakeholders and that their involvement in the process is minimal. Therefore, these groups could be the main providers of information necessary for analysis, regulators or providers of company objectives (decision making values).

This is why these stakeholders may be assigned temporality in the validity of the public keys. This validity can be considered for the time that the process lasts or/and the time that the employee performs functions related to the RMP or if is a member of the organization.

RMP promotes a constant and sequential analysis that allows maintaining traceability of the process. As well as a ledger that maintains a history of data, processes and ideas. This proposal is for the duration of the project and its specific objectives. However, when monitoring presents new evidence and results that need to be considered, the process can continue and start over with updated data. In addition, the temporality of the previous data will not be discarded, on the contrary, they can be used as inputs and be considered for new statistical data.

6.2.2 How could the information be shared outside the RMP blockchain and prevent work stealing?

As previously explained, the application of PKI in the blockchain allows the identification of the intellectual creator, in this way it is expected to minimize plagiarism. However, if someone needs to print the information, the system could allow the creation of a *read-only* document in PDF format to print. This document can then be shared with users outside the blockchain.

When the PDF is created, the document will contain the mixHash of the block and be visible when the document is printed. If the validation of the mixHash is required, then the user has to go back to the blockchain and locate the block, compare the mixHash to find the correct block, and then all the signatures of the contributor would be visible.

6.2.3 What could the system offer, and why is it recommended to be used?

Among the reasons for using a system that promotes generic and complete RMP, are the added values that help make the information as fluid and understandable as possible. The following describes the characteristics and its value of this system:

- Generic RMP: the system promotes a recursive, sequential and complete process that can be modified according to risk-related factors and the project needs. It also has different templates that can be used for different stages
- Visibility, traceability and proof of ownership: it has everything visible to the participants, it is easy to trace and allows the identification of the creators of the work
- Identification and certification of stakeholders: the system allows stakeholders to work in the system according to their level of power, interest and participation in the risk-related process. Everyone has to be certified and validated to operate the system
- Process-Ledger Protection: the system uses a limited consensus technology with the supervision of an external consultant, which creates a database usable in the future. Where other stakeholders contribute and become part of the protection technology with their IT resources. This collaboration implemented the protection of PKI
- Limited consensus technology: refers to the agreement/consensus for the null or partial modification of the ledger, tracking the owner of the information, owner of the modification and consensus transactions for related stakeholders in different stages or threads
- Adaptation of the block architecture: the generic blockchain architecture, can be adapted to the need of the risk management process. That includes different templates adaptable to various stages

- Blockchain Process: this architecture represents the risk communication and information flow through blockchain technology suitable for security and risk management. In addition to promoting the visibility of the intellectual authors of the ideas
- Multi-stakeholders Hash-security integration to the block architecture: this will ensure the agreement in the related information at the level of members of organizations, stakeholders, and other participants in the risk and safety management process. The multi-hash technology is linked with proof of ownership at all times
- Wallet Vault Technology: provides services for the creation of a digital wallet in which users manage their public keys and digital certificates

Apart from all the characteristics described, this system expects to be a useful tool that supports the decision-making process. The consideration that decision-makers are not the only ones with the capacity to make decisions, but that they are also the main providers of the companies' objectives, will include them from the beginning of the project. In this system, it is promoted that RMs can also decide in the process, not only carry out a risk assessment that will later be used for decision analysis. Therefore, decision-makers are expected to actively participate in the process and the RMs.

Due to these considerations, the system will allow observing the decisions that have been made during the process. In this way identifying what was the nature of the problem, what are the uncertainties, what were the objectives or if the objectives are adequate, and the early visibility of the necessity of trade-offs; among other considerations and the final decisions.

Another advantage is that all the initial considerations and the decisions are reflected by involving the decision-makers from the beginning. This is considered since, in some cases, it is challenging to keep track of the decisions that people have made because

> "when they have made a decision, people don't even keep track of having made the decision or forecast. I mean, the thing that is absolutely the most striking is how seldom people change their minds. First, we're not aware of changing our minds even when we do change our minds. And most people, after they change their minds, reconstruct their past opinion—they believe they always thought that" (Schrage & Kahneman, 2003)

This system proposes to avoid this loss of information and decisions and can identify the individual behind that, which will facilitate audits and/or recognise possible biases that could improve the system.

6.3 Security

6.3.1 Security issues

The following section will describe the risks that could happen to the system. Even though blockchain and PKI are robust systems that are difficult to tamper with, it is still not immune

to cyberattacks and fraud. These can be separated into three risk categories – *control, process, and technology* (Arunkumar & Muppidi, 2019).

The control aspect is risks related to how the system is being operated and controlled by humans. Some of the risks are:

- Decision-making is at the risk of exploiting fraud. Since a central authority controls the identification system, it can create a lack of trust in the decision-makers
- Controlled access could influence who can have a say in the RMP. The RM's controls the accessibility of the amount of influence a user can have
- Legal issues can be a problem because of how the data is shared on the chain. There could be some tasks that require sensitive information that could go against the GDPR (Vatra & Jiroveanu, 2010)
- Established trust toward the system. Trust to the provider, controller, the keyholders. To keep the trust of the users that their information is secure.
- The risk of losing the wallet and the keys. If the wallet is stolen, the thief has access to the blockchain and would be able to see the data stored, who is working there, and can attack within the system

The process aspect considers the risks that are associated with the interaction with the system and with the architecture and could be as follows:

- The access management, only the participants, assigned to the RMP have the permission to access the system and have been certified. If outsiders have somehow gained access, they have the opportunity to attack it from the inside
- Secure communication from users computers to the server; thus, the system operates in the correct order. However, since the communication is going from the server to external computers, it can lead to a risk that attackers will mislead the connection
- Untested code that is implemented can create an unwanted opportunity for hackers to gain access to the system. e.g. If an update to the system is uploaded, but its functionality has not been tested, it could make a trap door where attackers can bypass the security features
- The infrastructure of the blockchain can be developed with an unknown breach. For example, when implementing a new system or updating a part of the system, there could be undiscovered fail. This could happen in the new system, or a new function is in dispute with the old system functionality. This could lead to reduced functionality that could be exploited, making it weaker against attacks

The technology aspect considers the risks that are associated with the technical part of the blockchain and could be:

- Key Management considers how the system handles the expired, revoked, renewed, or certificated key. The risk concerns the keys are being leaked; the expired keys are not removed, renewal of the wrong key
- The risk of the smart contracts being used for malicious deeds. The smart contracts could be programmed with faults, or they could be programmed to attack the blockchain or its users

- Removing the users from the blockchain. This could create a risk for the consensus method, by removing users as a result, the specific criteria needed no longer can be met
- How to handle a user that is offline when voting is needed. This can prolong the functionality of the system

6.3.2 Cyberattacks

Here will be explained some of the cyberattacks that could happen to a blockchain and PKI, but is not limited to. However, it is worth mentioning that since the system does not operate with currency, these risks are not considered a threat to the proposed architecture. But, it is considered that attackers would try to get personal or confidential information about the companies.

Sybil attack is when hackers create false profiles on a network to control it. With the increase of accounts control by one person or a group, they influence the selection process of transactions that are going through. In blockchain technology, the famous 51% attack can be a Sybil attack, where the attacker controls the majority of the system computation power or user number. This would give full control of the system.

Routing attack is where an attacker interrupts the message before it reaches its end destination. Since the users are sending the block to the server, there is an online connection. The attacker would intercept the block before it would be uploaded to the server. At that point, the attacker can see the information sent, which can be confidential in the worst case. When they are "done", they can upload it again, without the system administrator can see that there has been an interaction.

Phishing attack focuses on stealing people passwords or wallets, so they can get access to the blockchain and interact with that user identity. The most common method is to send an email with a link to a website, where the user has to log in to renew their password. This is a false site and when they enter their information, the attacker gains the credentials information.

Hacking the servers or computers to gain information. Hacking the computer is to gain the information to access the blockchain, like the phishing attack. Hacking the servers is to gain all the users' credentials as well as data stored on the chain. If the server is hacked the attacker has access to it and can control everything.

Distributed Denial-of-service attack (DDoS) is where an attacker is overflooding a system with messages. The intention is to overload the system so the honest workers cannot upload their work, due to the reduced response time of the system. They could focus on a specific part of a system so it would not work and increase the functionality of other parts controlled by a malicious person.

Man-in-the-middle is where the attacker intercepts a message between two users. It is similar to the routing attack but is working by tamper the data between users. So if a block needs multiple users to be completed, one would have to be the template leader, and the other users

will have to send the information to him/her. Man-in-the-middle would interact in this message and be able to influence the data that is being sent.

DNS Attack is trying to get the users to connect to the attacker's counterfeit network. They are redirecting the blocks to a false network to gain the users' information. The counterfeit network has the same appearance as the real blockchain but has only changed the IP address. These can be hard to discover for a user since it is just like uploading to the chain.

Eclipse attack is where the attacker tries to isolate other users from the legitimate network and gain control over them without knowing it. If the attacker is successful, they control the input and the output messages that the users see and influence what the honest user can do.

6.3.3 Is the architecture safe enough for adding a block to the blockchain?

The PKI and blockchain technology combination create a network with high security, high transparency (for invited members or be able to recall from printed reports), high identification rate of the users, great tamper-proofing, and high protections of the users work, and fast and easy interaction. The proposed architecture increases the difficulty for some attacks to happen, like the Routing and Man-in-the-middle attack, since the data is linked to a specific user when sending it. It is not possible to edit these parts because of the linked function.

The consortium network and the PKI make Sybil attacks harder since the attacker needs to access the chain and create false identities to interact with the blockchain. If they get in the positions where they can make a Sybil attack, they have access to the server and would have taken over the internal and external CA servers before they would be able to create the accounts.

The system's biggest problem is the theft of wallets and identities. A prevention method that could be done to regain control of the system is to put compromised user wallets out of working condition. However, if the system is compromised, the trust in the system is lost, and all the information of the users and the blockchain can be searched.

For submitting the blocks and working in the templates, the system has high security that is safe enough to upload blocks. However, this system is only suitable for private networks and consortium networks; it needs user control. The PKI secure the users, then the Proof-of-ownership knows everyone who has contributed; the hash function's complexity increases the tampering security and creates a proper way of conducting RMP.

7 Conclusion

Blockchain technology allows to maintain an immutable and visible record book, but the identification behind each transaction is still a limitation. Its best-known use is Bitcoin; however, this technology is used in different areas. Therefore, one of its uses is expected to be adaptable to risk management with increased traceability and security to identify the owner behind the transactions. In order to start with this proposal, it was necessary to visualize a system that is dominated by three aspects, risk management as a process, blockchain as the technology to be used, and public key infrastructure as an identification infrastructure.

Risk management was considered as a continuous process of five stages that contain sequential and repetitive steps. Taking this into consideration, the risk identification process was used as a generic and adaptable basis for the rest of the stages.

Blockchain is a complex technology that is based on three layers, the blockchain technology, the protocol and the token and also considers the network adaptable for the specific need. All the layers present diverse technologies, that together make this a useful ledger for storing information in an immutable way.

The public key infrastructure is also a set of technologies that provides security through the implementation of a pair of keys, making it compatible with blockchain. For the implementation of a method to recognize the identity of the creators of the information, a central authority and cryptography combination was necessary.

For the development of this risk management blockchain, it was identified that not all stakeholders participate actively in the process. Those most involved in the risk management process are the risk managers, with high power and high interest. Other stakeholders are IT project managers and the central authorities, especially the ones that fulfil the data processor responsibility. The IT project managers, despite not having high power in the risk management process, are in charge of the combination of technologies and must be aware that a minimum error can cause failures to the process. Meanwhile, the central authority does not have high power in the risk management process either, but it oversees processing information and verifying identities.

A model for a generic architecture, that is adaptable not only to the process and its stages but also to the recursion of its steps, was proposed. This architecture combines blockchain and public key infrastructure, where blockchain serves as an important stage of the risk management process, risk communication.

A consortium network was proposed to be able to give access to the required users. In addition, it includes the implementation of a central authority that is responsible for certifying users, issuing identity certificates linked to their pair of keys and validating the owner of the keys. It will also be the one that will grant the process a pair of keys that will be managed solely by the

central authorities. On the other hand, the user will get a wallet on the server where their public keys and their certificates can be stored.

Blockchain technology has been modified to include the credentials of the users and creators of the work. Therefore, in the account state, the public key will be added to be able to link the information with the writer. In the transaction, only the nonce will be considered from the original structure, the address will be the risk management process address, the value will be replaced by the required information and the signature(s) will be the digital signature(s).

For the visualization of the blocks, two layers were considered. The front page will allow the visualization of the information with easier navigation through the use of templates. Meanwhile, the data page will contain the data to validate the uploaded information and the author of it.

Therefore, the proposed architecture answers the problem question

How risk identification process could be framed using blockchain, which improves the traceability, proof-of-ownership, and decision making of the interested parties without compromising their protection?

It was viable to outline an architecture suitable for risk management and each of its stages, steps, and tasks. In the study case, the risk identification stage proposes four steps with tasks that must be completed before proceeding to the next step. The system could also recognize the order of the process and the necessity to complete previous tasks before moving forward.

The use of blockchain in the risk management process will allow the *revocation of intermediaries* when sharing information. It also has *shared write access* for users who can view and provide information. This technology allows complying with adequate risk communication that will be carried out through consensus and agreements by all those involved. This is a very useful tool to *verify* and make *visible* the decisions made in the process, thus *supporting trust* between the parties.

Another feature that blockchain and the system share is the *storage of non-transaction data in large quantities*. The proposed system, in addition to saving the data, was adequate so that the data can be linked between steps and stages. Therefore, *connectivity* based on the exposed knowledge is promoted.

The creation of the layers of the system allows the collaborative work in the same block. The new *proof of ownership* protocol allows the user to upload the information to the block and this information is signed by its authors. This represents the *agreement* of the information by all participants.

This proposal has a *functional control* that will be decided by the company and its need. The *consortium network* may limit the participants in the process and may decide the level of visibility, whether visibility is required for the entire company or clearly for stakeholders.

Furthermore, it was feasible to use the public key infrastructure to improve *traceability, security* and *authentication* of the users. The implementation of the *certificated pair of keys* allows signing automatically the written information. Also, to have a quick identification in the block since the name of the authors and the organization identification to which they belong will be presented in the front layer.

To not compromise the *protection of users*, it was possible to include central authorities to *certify and authenticate the keys* used. The certificates issued by them will verify the validity of the keys and therefore to identify the rightful owner. In addition, the central authority will be the carriers and controllers of the pair of keys created for the process, these will only allow the asymmetric decryption when it is necessary to verify the immutability of the information.

RMP was considered as an *ongoing process* in which several people are involved and their collaboration is required in some stages. Consequently, the two layers blockchain will allow working on a block/template before the final block is uploaded to the chain. Furthermore, if any modification and improvement are required, the solution was to *reach a consensus* through the practical byzantine fault tolerance.

Furthermore, advantages were identified for both the process and the users. By having a generic risk management process combined with blockchain and public key infrastructure, it will provide *immutability, integrity and no repudiation* of the participants and their work. Another advantage is that there will be constant and visible communication, with the expectation of no loss of consensus, agreements and decisions in the process and the blockchain. This will help decision-makers to base their decision on complete and reliable information.

Despite being a robust system with complex technologies, there are still security issues that could not be avoided. The remnants are the theft of the wallets and identities, and the hacking of the central authorities server.

Finally, this system has succeeded in proposing a system with security, transparency, identification and protection of users and their work, tamper-proofing, visible communication, agreement, and easy interaction.

8 Further work

The following topics describe further research that is beneficial for the proposed architecture to ensure optimal functionality and security.

- To perform a physical development of the system. This means to code the system to make a functional program. With ~~a~~ physical and interactive system, further research would be able to perform based on data
- When the architecture has been programmed, the other stages in RMP and more templates can be developed
- The system can be tested several times. These tests could be related to blockchain and/or PKI to find faults in the system. Also, it could be used to improve cybersecurity
- Further research on the risks could help increase the robustness making it more resistant to attacks. When an attack happens, a plan developed on how to cope with the damages would be beneficial to the systems resilience and the trust of the user acquiring the system
- When considering the user, more detailed information on how the wallet could be stored should be considered. Different kinds of storage for the wallets and how the user interacts with it could create a more widely usage for the application

9 References

101 Blockchains. (2020, June 29). When To Use Blockchain Technology? *101 Blockchains*. https://101blockchains.com/when-to-use-blockchain/

Adams, C., Lloyd, S., & Adams, C. (2003). *Understanding PKI: Concepts, standards, and deployment considerations* (2nd ed). Addison-Wesley.

Ahmady, G. A., Mehrpour, M., & Nikooravesh, A. (2016). Organizational Structure. *Procedia - Social and Behavioral Sciences*, *230*, 455–462. https://doi.org/10.1016/j.sbspro.2016.09.057

Anand, A. (2019, December 9). *Breaking Down: SHA-3 Algorithm*. Medium. https://infosecwriteups.com/breaking-down-sha-3-algorithm-70fe25e125b6

Antonopoulos, A. M., & Wood, G. (2018, November). *Mastering Ethereum*. https://www.oreilly.com/library/view/mastering-ethereum/9781491971932/ch04.html

Ariwa, E., & El-Qawasmeh, E. (Eds.). (2011). *Digital enterprise and information systems: International conference, DEIS 2011, London, UK, July 20 - 22, 2011 ; proceedings*. Springer.

Arunkumar, S., & Muppidi, S. (2019, July 18). How to Secure your Blockchain Solutions. *IBM Developer*. https://developer.ibm.com/articles/how-to-secure-blockchain-solutions/

Badratdinov, T. (2018, November 29). *Blockchain Explained—Kauri.io*. https://kauri.io/#communities/Getting%20started%20with%20dapp%20development/blockchain-explained/#hashing

Binder, J. C. (2002). *Introduction to PKI - Public Key Infrastructure*. http://www.k-binder.be/Papers/PKI_V11.pdf

Cenek, M., & Částek, O. (2016). A Survey of Stakeholder Visualization Approaches. *Central European Journal of Management, 2*(1,2). https://doi.org/10.5817/CEJM2015-1-2-1

Datatilsynet. (2021). *Datatilsynet*. Datatilsynet. https://www.datatilsynet.dk/

Downey, L. (2021, October 6). *What Is an Algorithm?* Investopedia. https://www.investopedia.com/terms/a/algorithm.asp

Dr. Wood, G. (2021). *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*.

European Commission. (2018). *Data protection in the EU* [Text]. European Commission - European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

European Union. (2016). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1489-1-1

Folketinget. (2016, November 29). *Sådan arbejder regeringen*. Folketinget. https://www.ft.dk/da/folkestyret/regeringen/saadan-arbejder-regeringen

Forsvarsminiseriet. (2020, August 17). *Cybersikkerhed*. Forsvarsministeriet. https://fmn.dk/da/arbejdsomraader/cybersikkerhed/om-cybersikkerhed/

Frankenfield, J. (2021, October 8). *What Is a Crypto Token?* Investopedia. https://www.investopedia.com/terms/c/crypto-token.asp

Galston, E. (2021, June 16). Opinion | Untraceable Bitcoin Is a Myth. *Wall Street Journal*. https://www.wsj.com/articles/untraceable-bitcoin-is-a-myth-11623860828

Genesis Devcon. (2018, December 21). *What are Blockchain Protocols and How Do they Work? | by Genesis DevCon | Medium*. https://medium.com/@genesishack/draft-what-are-blockchain-protocols-and-how-do-they-work-94815be5efa7

Gwyneth, I. (2021, January 31). Top 5 Enterprise Blockchain Protocols. *101 Blockchains*. https://101blockchains.com/blockchain-protocol/

Haber, S., & Stornetta, W. S. (1991). How To Time-Stamp a Digital Document. In *Journal Of Cryptology* (Vol. 1991).

Hooda. (2019, January 11). Practical Byzantine Fault Tolerance(pBFT). *GeeksforGeeks*. https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/

ISO 73. (2009, November). *ISO Guide 73:2009(en), Risk management—Vocabulary*. https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

ISO 31000. (2018). *ISO 31000:2018(en), Risk management—Guidelines*. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

ISO 31010. (2009). *Risk management—Risk assessment techniques Final Draft*.

Joint Committee of Structural Safety (JCSS), F. & MH. (2008). *Risk assessment in engineering*. Joint Committee of Structural Safety.

Kim, S., Deka, G. C., Rathee, P., Gatteschi, V., Lamberti, F., Demartini, C., Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R. C., Michelin, R. A., Zorzo, A. F., & Kanhere, S. S. (2020). *Advanced applications of blockchain technology*. Springer.

Marco Polo Network. (2018, January 30). *The Difference Between Blockchain and Distributed Ledger Technology*. Marcopolonetwork.Com. https://www.marcopolonetwork.com/articles/distributed-ledger-technology/

Martin, M. (2021, November 9). *Difference Between Encryption and Decryption*. https://www.guru99.com/difference-encryption-decryption.html

Nakamoto, S. (2008). *Bitcoin: A peer-to-Peer Electronic Cash system*.

Oxford Dictionaries. (2021). *protocol noun—Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com*. https://www.oxfordlearnersdictionaries.com/definition/english/protocol?q=Protocol

Oxford University. (2021a). *interest_1 noun—Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com*. https://www.oxfordlearnersdictionaries.com/definition/english/interest_1?q=interest

Oxford University. (2021b). *involvement noun—Definition, pictures, pronunciation and usage notes | Oxford Advanced American Dictionary at OxfordLearnersDictionaries.com*. https://www.oxfordlearnersdictionaries.com/definition/american_english/involvement

Oxford University. (2021c). *power_1 noun—Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com*. https://www.oxfordlearnersdictionaries.com/definition/english/power_1

Penard, W., & Werkhoven, T. van. (2007). *On the secure Hash algorithm family*.

Rangel, J. (2020, March 26). *Course: Risk Analysis. Master in Risk and Safety Management*. Basic Definitions, Aalborg University, Esbjerg Campus.

Rausand, M. (2011). *Risk assessment: Theory, methods, and applications*. Wiley.

Rodriguez, N. (2018, December 27). ¿Necesitas una blockchain? Árbol de decisión de blockchain definitivo. *101 Blockchains*. https://101blockchains.com/es/necesitas-una-solucion-blockchain/

Schrage, M., & Kahneman, D. (2003). *Daniel Kahneman: The Thought Leader interview*. Strategy+business. https://www.strategy-business.com/article/03409

Statista. (2021). *Number of crypto coins 2013-2021*. Statista. https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

Tardi, C., & Rasure, E. (2021, July 2). *Genesis Block Definition*. Investopedia. https://www.investopedia.com/terms/g/genesis-block.asp

Team Kaccak. (2021). *Keccak Team*. https://keccak.team/keccak.html

The Guardian. (2021, October 5). Facebook explains error that caused global outage. *The Guardian*. https://www.theguardian.com/technology/2021/oct/05/what-caused-facebook-whatsapp-instagram-outage

Trcek, D. (2014). *Managing Information Systems Security and Privacy*. Springer Berlin.

Vacca, J. R. (Ed.). (2004). *Public key infrastructure: Building trusted applications and Web services*. Auerbach Publications.

Van den Berghe, L. a. A., & Levrau, A. (2004). Evaluating Boards of Directors: What constitutes a good corporate board? *Corporate Governance: An International Review*, *12*(4), 461–478. https://doi.org/10.1111/j.1467-8683.2004.00387.x

Van Hijfte, S. (2020). *Blockchain Platforms: A look at the underbelly of distributed platforms*. Morgan & Claypool Publishers.

Vatra, N., & Jiroveanu, D. C. (2010). RiskManagement in Public key Infrastructure. In *Review of international Comparative management*.

Wakefield, J. (2021, October 5). What happened to Facebook, WhatsApp, and Instagram? *BBC News*. https://www.bbc.com/news/technology-58800670

Wedell-Wedellsborg, T. (2017, January 1). Are You Solving the Right Problems? *Harvard Business Review*. https://hbr.org/2017/01/are-you-solving-the-right-problems

Wilkie, A. M., Christina. (2021, June 7). *U.S. recovers $2.3 million in bitcoin paid in the Colonial Pipeline ransom*. CNBC. https://www.cnbc.com/2021/06/07/us-recovers-some-of-the-money-paid-in-the-colonial-pipeline-ransom-officials-say.html

Zhang, D., Le, J., Lei, X., Xiang, T., & Liao, X. (2021). *Exploring the redaction mechanisms of mutable blockchains:Acomprehensive survey*.

Zhang, S., & Lee, J.-H. (2020). Analysis of the main consensus protocols of blockchain. *ICT Express*, *6*(2), 93–97. https://doi.org/10.1016/j.icte.2019.08.001

10 Appendix

10.1 Generic Risk Management Process

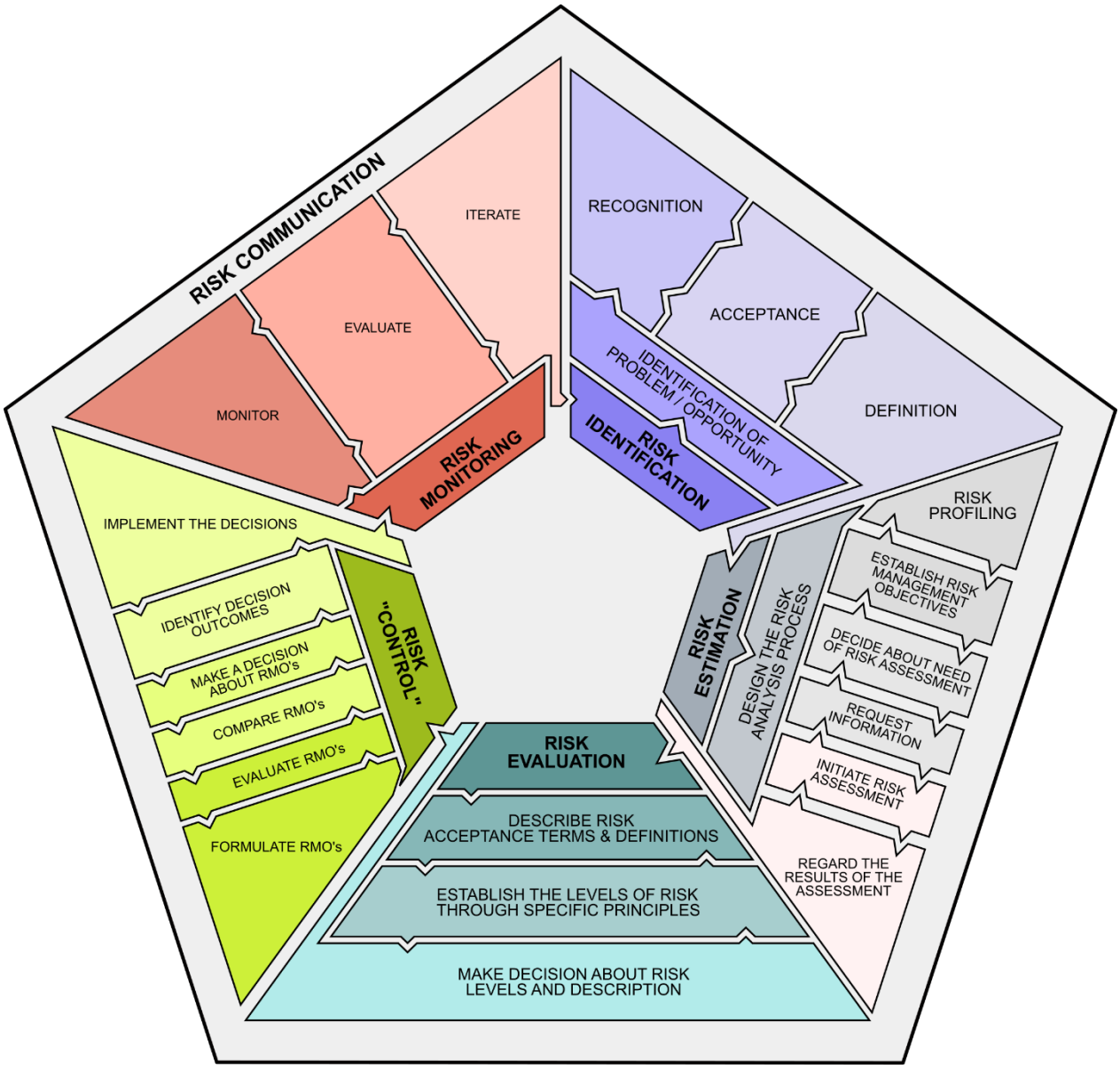


Figure 53 Complete Generic Risk Management Process (Rangel, 2020)