# MASTER'S THESIS

## Blockchain-based systems: What are the risks to the stakeholders?

Meulemans-Rangel Maia, D.

**Award date:**
2022

# Blockchain-based systems: What are the risks to the stakeholders?

| | |
|---|---|
| Opleiding: | Open Universiteit, faculteit Betawetenschappen |
| | Masteropleiding Business Process Management & IT |
| Degree program: | Open University of the Netherlands, Faculty Science |
| | Master of Science Business Process Management & IT |
| Course: | IM0602 BPMIT Graduation Assignment Preparation<br>IM9806 Business Process Management and IT Graduation Assignment |
| Student: | Daniela Meulemans-Rangel Maia |
| Identification number: | |
| Date: | 16/01/2022 |
| Thesis supervisor | C.J. Tesselhof MSc MSc |
| Second reader | dr. ir. G.L.S.G. Janssens |
| Version number: | FV2 |
| Status: | <draft/~~final version~~> |

# Abstract

The development in the utilization of Blockchain-based systems (BBS) is compared with the internet development in the early ’90s. In order to accelerate the adoption of the BBS, awareness of its risks should be developed. Even though previous studies have identified stakeholders and risks of BBS, there was no sufficient research associating the risks to the stakeholders. The work performed in this dissertation focused on filling this gap. It includes empirical research that has identified stakeholders and risks of BBS, confirming some results of previous studies.

Additionally, it has contributed with a framework, associating the risks to the stakeholders. The framework is developed using the template analysis technique to classify stakeholders and risks identified into categories. This research contributes to the research community by providing empirical research that extends the body of knowledge showing associations of the risks by stakeholders’ types involved in a BBS. This study also contributes to practitioners by providing the framework that can be used as guidance for risk assessments per type of stakeholders in a BBS.



# Key terms

Blockchain-based systems, risks, stakeholders

# Summary

The development in the utilization of Blockchain-based systems (BBS) is compared with the internet development in the early ’90s.

Blockchain-based systems are a decentralized network where transactions can be executed and where the Blockchain technology, a form of distributed ledger technology, is deployed. (Butijn et al., 2020, Tesselhof et al., 2020).

In order to accelerate the adoption of BBS, risk awareness may assist the stakeholders in the process of BBS’s adoption. Previous research papers have identified a variety of stakeholders and several risks of BBS. However, the association of the risks to the stakeholders involved in a BBS has not been extensively researched. The work performed in this dissertation focused on filling this gap. The main research question is therefore stated:

**“What are the risks to the stakeholders involved in a BBS?”**

In the first instance, a literature review is conducted to find definitions for BBS and identify stakeholders and risks that have been disclosed in previous studies. The results of the literature review revealed several stakeholders and risks. Only one research addressed the intersection between risks and stakeholders. The literature review also demonstrated that the research papers did not use standard categorization for the identified stakeholders and risks. Each study revealed a different classification for the identified stakeholders and risks.

Subsequently, the empirical research is designed with the goal to identify stakeholders, risks, and risks to the stakeholders. Therefore, the empirical research stated the following research questions: i) what are the stakeholder of BBS; ii) What are the risks of the BBS and the third and main research question iii) What are the risks to the stakeholders involved in a BBS? The empirical research is designed as a qualitative survey, using semi-structured interviews for the data collection. The data analysis is performed jointly with a research group to avoid individual bias. Additionally, categories templates were developed using the template analysis technique to create a basis for a standard categorization of all the stakeholders and risks identified during the research.

The first research question is answered disclosing 39 stakeholders identified during the empirical research and classified into six categories: technical stakeholders, political Stakeholders, process stakeholders, investors, social groups, and others. The answer to the second research question shows 33 risks identified during the empirical research, classified into eight main categories: Criminal use, technical, privacy, legal, human, financial, business case, and economic risks.

The answer to the third and main research question uses the framework built, which displays the associations between stakeholders and the related risks. It combines the results of the first two research questions and the associations made between the stakeholders and their related risks, according to the view of the interviewed stakeholders.

In summary, the empirical research has identified stakeholders, risks, and risks to the stakeholder of a BBS.

The contribution of the current work to the research community is twofold. First, it has identified additional stakeholders and risks related to the BBS. Second, it created a framework that provides associations between the risks and the stakeholders involved in a BBS.

This study also contributes to practitioners, who may use the resulting framework for guidance on risk assessments related to BBS stakeholders and their related risks.

# Contents

# 1. Introduction

## 1.1. Background

Blockchain is emerging as a potentially disruptive technology, which uses a decentralized ledger that facilitates peer-to-peer value transfer (Frizzo-Barker et al., 2020). Blockchain is the underlying technology behind Bitcoin (Nakamoto, 2008), the most famous application of the blockchain technology.

Swan has categorized the development of the blockchain technology into three different categories. The first one is related to the applications in the payments systems and cryptocurrencies (Blockchain 1.0), followed by applications in finance, making possible the transfer of all kinds of financial assets through smart contracts (Blockchain 2.0). The third type of applications, beyond finance, applications in various business domains (Blockchain 3.0) such as government, health, arts and culture. (Swan, 2015, in Frizzo-Barker et al., 2020, p. 1).

Viriyasitavat and Hoonsopon (2019) argued that blockchain-based systems ( the author used the term blockchain only) have the same characteristics as business processes. Alles and Gray (2020) consider blockchain technology as part of a broader business process and stated that "blockchains are means towards an end and not an end in themselves." Blockchains could be understood as new global systems that operate like the Internet."(Tasca & Tessone, 2017, in Pillai, Biswas, & Muthukkumarasamy, 2020). Many information infrastructures in the future will be built based on such decentralized networks using blockchain technology (Bahri & Girdzijauskas, 2019; Zheng et al., 2017, in Pillai et al., 2020).

Even though this technology is promising and considered disruptive, its broader implementation is hindered by the lack of trust in the technology, which is considered a human barrier to its adoption (Schlegel, Zavolokina, & Schwabe, 2018). Siegrist and Cvetkovich (2000) argue that when lacking the necessary knowledge, most people are not able to evaluate risks, and therefore risk assessment is delegated to trusted experts.

Various blockchain-related research papers have focused on investigating the risks of blockchain-based systems (BBS). Prewett, Prescott, and Phillips (2020) have demonstrated a broad list of risks associated to the adoption of the BBS: Design, endpoint, data security, smart contracts, storage, compliance, vendor, contractual and private-key management risks. However, they have mainly focused on the consortium type of BBS within the business-to-business context. Zetzsche, Buckley, and Arner (2018) have discussed the liability risks of BBS however have performed their analysis considering risks only from a legal point of view. Cagigas, Clifton, Diaz-Fuentes, and Fernandez-Gutierrez (2021) identified risks in the view of stakeholders, however only in the context of the public services domain. No research has presented a stakeholders-centric approach, specified by stakeholders' roles and associated risks.

This research aims to fulfill this gap. The goal is to provide practitioners and academics with a risk overview per stakeholders' type involved in a blockchain-based system.

## 1.2. Exploration of the topic

### 1.2.1. Blockchain-based systems (BBS)

The term blockchain-based system (BBS) is not broadly used among researchers, who often refer to other terms such as blockchain, blockchain networks, and blockchain technology, meaning the blockchain-based systems.

Viriyasitavat and Hoonsopon (2019) defined blockchain as "a technology that enables immutability, and integrity of data in which records of transactions made in a system are maintained across several distributed nodes that are linked in a peer-to-peer network." According to Jaoude and Saade (2019), blockchain refers to a decentralized transaction data management technology. In a blockchain-based system, transaction data is processed into blocks by miner nodes, and all blocks are linked together via hash operations (Zhang, Zhong, Wang, Chao, & Wang, 2020). Butijn, Tamburri, and Heuvel (2020) suggest that blockchain networks can be classified according to their accessibility and permissions.

Regarding accessibility, blockchain networks can be classified as public, private or consortium. Regarding permissions, blockchains networks can be classified as permissionless or permissioned.

**Public blockchains:** like Bitcoin or Ethereum, participation is open to anyone who can access and read any data related to any transaction in the blockchain (Nanayakkara, Perera, & Senaratne, 2019). Public BBS have technical limitations such as privacy and scalability (X. Xu et al., 2017).

**Private blockchains:** only approved members can join the network (Calderón & Stratopoulos, 2020)

**Consortium blockchains:** are partially private; each participant belonging to one organization and the group of all organizations participating in the network is called a consortium (Calderón & Stratopoulos, 2020).

**Permissionless blockchains:** allow anyone to validate the ledger's integrity by running consensus mechanisms (Viriyasitavat & Hoonsopon, 2019).

**Permissioned blockchains are** where ledgers are shared and validated by the predefined group of nodes or members (Viriyasitavat & Hoonsopon, 2019).

Blockchain technology can be classified as inter-organizational systems (Werner, Basalla, Schneider, Hays, & Vom Brocke, 2021). Inter-organizational systems allow information to be exchanged across organizational boundaries (Werner et al., 2021).

### 1.2.2. Stakeholders

"Stakeholder" is a term that has been differently defined by many researchers, reflecting their own perspectives and according to the different types of stakeholders they deal with (Pouloudi, 1999).

Freeman has defined stakeholders in the strategic management domain as "any group or individual who can affect or is affected by the achievement of the organization's objectives" (Freeman, 1984, as cited in Pouloudi, 1999, p. 2). Pouloudi (1999) has extended Freeman's stakeholder definition to the context of interorganizational systems. Interorganizational systems allow information to be exchanged across organizational boundaries (Werner et al., 2021). As BBS can be classified as interorganizational systems (Werner et al., 2021), it is appropriate for this research to adopt the stakeholder definition made by Pouloudi, who suggested that "A stakeholder of an inter-organizational system is any individual, group, organization or institution who can affect or be affected by the interorganizational system under study."(Pouloudi, 1999, p. 8).

### 1.2.3. Risk

"Risk is the probability of occurrence of an event that has some consequences" (Kliem, 2000). Risk assessment is, however, not an easy task. Most laypeople do not possess detailed knowledge for a rational assessment of risks associated with complex technologies and rely on experts or authorities' opinions when risk assessment is needed (Siegrist & Cvetkovich, 2000).

## 1.3. Problem statement

There are various research performed focused on the risks of the BBS. Some authors focused on risks of the BBS such as network risks, double spending attack risks, private key risks, and smart contracts risk (Morganti, Schiavone, & Bondavalli, 2018), security risks (Daramola & Thebus, 2020), Denial-of-service risk (Q. Xu et al., 2018) and risks of forking (Yeung & Galindo, 2019). These risks are related to the network and its vulnerabilities to attacks applied to any network user. These research papers have not included the stakeholders associated with the mentioned risks.

Prewett et al. (2020) have performed a comprehensive analysis on BBS risks, including: design, endpoint, data security, smart contracts, storage, compliance, vendor, contractual and private-key management risks. They have analyzed risks faced by professionals who have implemented BBS solutions. However, their research does not describe the stakeholders' types related to the discussed risks.

Cagigas et al. (2021) have identified risks of the BBS in the view of three types of stakeholders, limited to the public services domain (governments, citizens, and civil servants).

C. Lu, Batista, Hamouda, and Lemieux (2020) have performed a stakeholder-centric study in the personal health data sharing domain with the focus on exploring consumers' intentions and concerns. They have identified various risks to the users of blockchain-based personal data sharing: Cyber-attacks risk, risk of losing private-key and privacy risk due to the risk of malicious purpose in the use of the information by the third parties granted access to the data.

Research involving risks on the BBS so far has been mainly focused on the network risks of the BBS. Previous research has not focused on the stakeholders' types when discussing general risks. Studies that considered the stakeholders-view are limited to a few domains. There has not been any research that has had a stakeholders-centric approach presenting their associated perceived risks according to the different stakeholders' roles within the BBS.

Cagigas et al. (2021) have already identified the need for the diversity of empirical methods and empirical research on the BBS implementation to analyze real cases adoptions in the private and public sectors. This research aims to fill this research gap and present a framework that can be used as guidance for evaluating risks to the stakeholders when considering a future implementation of BBS.

## 1.4. Research objective and questions

The current research aims to identify the risks for the stakeholders involved in a BBS and has the following main research question:

**RQ: What are the risks to the stakeholders involved in a blockchain-based system?**

There are some sub-questions requiring clarification before answering the main research question:

i. What are blockchain-based systems?
ii. Who are the stakeholders of the blockchain-based systems?
iii. What are the risks of the blockchain-based systems?

It is expected that the answers to the sub-questions will explain the characteristics of BBS, identify the stakeholders and risks related to BBS. In this way, the literature review will provide a basis for the empirical research, where it is expected to collect the data related to the perceived risks to different types of stakeholders, compare it to literature, and answer the main research question.

## 1.5. Motivation/relevance

The current research concerns the identification of what are the risks to the stakeholders involved in a BBS. The goal is to build a framework where stakeholders can be associated with their related risks since, from the literature review, Cagigas et al. (2021) was the only research that has presented a stakeholders-centric approach and their associated risks. However, their research has focused only on the public services domain.

Before implementing a new technology, it is a natural need to understand its risks. Siegrist and Cvetkovich (2000) discussed the importance of social trust to judge new technologies' risks, benefits, and acceptability. Their study demonstrated that laypeople without specific knowledge of complex technologies rely on experts or authorities when forced to make risk assessments. Therefore, this research aims to contribute to practitioners who can use the framework as a guideline for risk assessment, per related stakeholders, when considering BBS use or future adoption.

This research aims to provide a twofold academic contribution. First, increasing the body of knowledge by providing diversified empirical research method within BBS, as suggested by Cagigas et al. (2021). Second, filling the gap in current research considering risks associated with stakeholders involved with blockchain-based systems.

## 1.6. Main lines of approach

This research continues in chapter 2, providing a literature review of prior research performed by identifying definitions for BBS, the related stakeholders, and the risks of the BBS. Chapter 3 describes the empirical research methodology and design. The results of the empirical research and the answers to the research questions are disclosed in chapter 4. The research is concluded in chapter 5, which includes a discussion of the findings, impact on the literature and proposals for future research.

# 2. Theoretical framework

This chapter includes details about the databases consulted, search queries performed, and the process to select the relevant literature for review. It also establishes the goals of the subsequent empirical research based on the findings from the literature reviewed.

## 2.1. Research approach

In order to answer the first three sub-questions of this research (as mentioned in section 1.4), a literature search is performed. It is conducted using the search engine of the Open University (OU) library, which provides access to articles from well-known databases such as Science Direct, Web of Science, SpringerLink, IEEE, among others. Google scholar is used in case articles were not available to be retrieved from the OU library.

Aiming to select articles that meet quality requirements for this master research and keep consistency with the search for all three research questions, a filter is applied to select only peer-reviewed journal articles and conference proceedings written in English. As the central research topic is BBS, it considered that this subject was only introduced to the research community upon the appearance of the white paper from Nakamoto (2008). Therefore, the period selection restricts publications from 2008 until March 31, 2021, when the search in the literature was performed. Publications after this date were disregarded.

The design of the search queries is described below. The keywords used to build the search derive from the initial literature review described in chapter 1.

**RQ1: What are blockchain-based systems?**

This search aims to identify articles that provide definitions for blockchain-based systems. The two keywords related to the search are “blockchain-based system,” “definition,” and related word variations, as included in Appendix 1. Considering that the word “definition” can be broadly used within the article, the search will be applied in the document's title and the abstract.

**RQ2: Who are the stakeholders of the blockchain-based systems?**

This search aims to identify articles that mention stakeholders of blockchain-based systems. The two keywords related to the search are “blockchain-based system,” “stakeholder,” and related word variations, as included in Appendix 1. As the word “stakeholder” can be broadly used within the article, the search will be applied in the document's title and the abstract.

**RQ3: What are the risks of the blockchain-based systems?**

This search aims to identify articles that mention the risks of the BBS. The two keywords related to the search are “blockchain-based system” and “risks” and related word variations, as included in Appendix 1. As the word “risk” can be broadly used within the article, the search will be applied in the document's title and the abstract.

The search string implemented per research question is presented in section 2.2.

Afterward, the relevancy of the articles that resulted from the search string will be analyzed and selected following the order: Title of the publication, abstract, and screening of primary content in the articles. Afterward, the identified relevant articles will be thoroughly read. The articles that contribute to answering the related research questions will be included in the results.

## 2.2. Implementation

In order to perform the literature search, the queries designed in the section 2.1 were implemented in this phase. The final search query applied per research question, and their respective results are included in Table 1.

Table 1: Final search query

| Research Question | Search string | Results | Excluded (1) | Excluded (2) | To be fully read | Used in literature review |
|---|---|---|---|---|---|---|
| RQ1 | ((TitleCombined:("blockchain-based system*")) OR (TitleCombined:(blockchain system*))) AND (Abstract:(DEFIN*)) AND ((Abstract:(blockchain-based system*)) OR (Abstract:(blockchain system*))) | 38 | -22 | -8 | 8 + 1(*) | 7 |
| RQ2 | ((TitleCombined:("blockchain-based system*")) OR (TitleCombined:(blockchain system*)) OR (TitleCombined:(blockchain network))) AND (Abstract:(stakeholder* OR actor*)) | 22 | -7 | -6 | 9 | 7 |
| RQ3 | ((TitleCombined:("blockchain-based")) OR (TitleCombined:("blockchain-based system*")) OR (TitleCombined:(blockchain*)) OR (TitleCombined:(blockchain system*)) OR (TitleCombined:(blockchain network))) AND (TitleCombined:(risk*)) | 38 | -16 | -11 | 11 | 9 + 1(**) |

| | |
|---|---|
| Excluded (1) | Excluded after reading the abstract |
| Excluded (2) | Excluded after screaning the articles |
| (*) | One extra article provided by the thesis supervisor has been included. |
| (**) | One article identified from the results of the RQ2 has been included. |

**Implementation research question 1: What are blockchain-based systems?**

The search query applied to this research question resulted in 38 articles. The articles have been analyzed per relevance to the research question. After identifying relevant articles, eight articles were selected to be entirely read. In addition to this query, one article provided by the thesis' supervisor has been included independent of the search query: Tesselhof, Kusters, Janssens, and Veuger (2020). Therefore in total, 9 articles were selected to be entirely read. Finally, a total of 7 articles were included in the literature review.

**Implementation research question 2: Who are the stakeholders of the blockchain-based systems?**

The search query applied to this research question resulted in 22 articles. The articles have been analyzed per relevance to the research question. After identifying relevant articles, nine articles were selected to be entirely read. Finally, a total of 7 articles were included in the literature review.

**Implementation research question 3: What are the risks of the blockchain-based systems?**

The original literature search design for this research question (mentioned under section 2.1) has resulted in 296 articles. This total has not been considered feasible within the time constraint of this research. In order to bring the results to a manageable total of articles, the final query applied has included the keywords search only in the title of the document, as shown in Table 1 above. This last search resulted in 38 articles. The articles have been analyzed per relevance to the research question. After identifying relevant articles, 11 articles were selected to be entirely read, and from this total, nine articles were included in the literature review. The articles identified under research question 2

have also been screened in relation to risks seeking to identify papers that considered both risks and stakeholders. This search identified 1 article.

## 2.3. Results and conclusions

### 2.3.1. What are blockchain-based systems (BBS)?

Narayanan and Clark stated that “Blockchain is an umbrella term for a class of systems that share some of the characteristics of Bitcoin” (Narayanan and Clark, 2017, in Tran, Ali Babar, & Boan, 2021).

“Blockchain has not yet reached a widely accepted or easily understood definition in scholarship, much less in mainstream public discourse” (Frizzo-Barker et al., 2020). Birch, Brown and Parulava stated that “the term blockchain means too many different things to different people” (Birch, Brown, & Parulava, 2016, in Frizzo-Barker et al., 2020).

This research is focused on BBS. Various definitions encountered in the reviewed literature defined “blockchain” and “blockchain technology.”. Only two of the definitions found can be related to blockchain-based systems. Details of the literature review are presented in Appendix 2.

Tesselhof et al. (2020) have performed a systematic literature review with the objective to create taxonomy and definitions related to BBS. Their work is the only identified research that presented an explicit definition for BBS: “A decentralized network where transactions can be executed”(Tesselhof et al., 2020).

Butijn et al. (2020) research analyze the interconnected and interdependent systems part of the network where the blockchain technology is deployed. One of the results of their research is a definition for blockchain technology: “Blockchain technology is a form of distributed ledger technology, deployed on a peer-to-peer network where all data are replicated, shared, and synchronously spread across multiple peers”(Butijn et al., 2020, p. 13).

A semantic comparison between the concepts presented in the two definitions mentioned above is represented in figure 1.

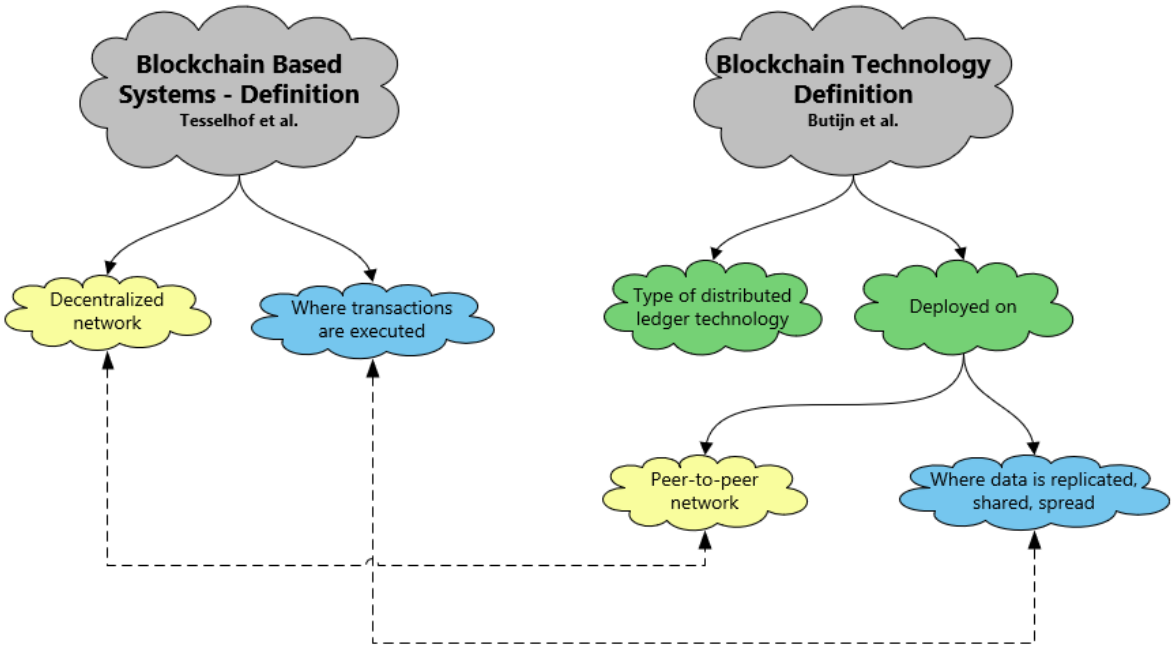



Figure 1 – Semantic comparison between concepts included in the definitions from Butijn et al. and Tesselhof et al.

The comparison between Butijn et al. (2020) and Tesselhof et al. (2020) is made with the objective to demonstrate that the research from Butijn et al. (2020) is relevant for this research for the following reasons: i) Their research focused at first instance on the blockchain technology; however, it has also identified aspects of the BBS. ii) It demonstrates that the taxonomy is still not aligned within the research community, and when analyzing additional papers, this should be considered. iii) Butijn et al. (2020) analyzed the blockchain technology which is deployed into BBS. Their research analyzed the BBS components, while Tesselhof et al. (2020) have focused on the taxonomy and definitions around BBS. As the research community is applying the concepts blockchain, blockchain-based systems and blockchain technology interchangeably, it is helpful to apply a combination of the two definitions in order to contextualize blockchain technology in relation to BBS, resulting in the following merged definition:

> Blockchain-based systems are a decentralized network where transactions can be executed and where the Blockchain technology, a form of distributed ledger technology, is deployed. (Butijn et al., 2020, Tesselhof et al., 2020).

### 2.3.2. Who are the stakeholders of the BBS?

Blockchain Technology is considered a "General Purpose Technology" (Davidson et al., 2016, in Unalan & Ozcan, 2020). Buth, Wieczorek, and Verbong (2019) argued that the current BBS development stage can be compared to the development stage in the use of the internet in the early '90s. Li, Greenwood, and Kassem (2019) made a similar comparison and highlighted that the BBS, compared to the internet, can potentially impact the whole society. The influence of BBS in the society is also disclosed in the network of actors' from Unalan and Ozcan (2020). The network of actors does not point out single stakeholders, rather groups of industries instead. However, it is helpful to understand that the entire society and all the sectors of the economy are potential stakeholders of the BBS.

Li et al. (2019) identified stakeholders within the construction domain, split into four domains: technical, policy, process and social. According to Li et al. (2019), the stakeholders included in the technical dimension deal with all technical aspects that a system requires to function; the policy dimension comprehends the stakeholders within the environment in which the BBS are inserted, such as regulations, laws, policies, standards, and compliance. The stakeholders included in the process dimension are related to all business practicalities related to the organization implementing the BBS. The social dimension is focused on the social impact and the integration with the real-world such as the effects of data protection regulations or environmental sustainability. It can be argued that the description of the dimensions proposed by Li et al. (2019) can be broadly applied and are not limited to the construction domain.

The present research is focused on identifying stakeholders of the BBS. The details of the literature reviewed are included in Appendix 3. Stakeholders' types that are clearly applicable only to one specific domain have not been included in the results. A list of the stakeholders identified in the literature review is included in Table 2, with the identified stakeholders presented into clusters. The clusters were displayed according to their similarities and for visualization purposes only, as not all the literature reviewed have used the same categories to present the stakeholders. The empirical research aims to identify stakeholders of BBS and verify if the results from the literature review are also confirmed empirically. Therefore, the same question will be subject to the empirical research: What are the stakeholders of the BBS?

Table 2 - Blockchain-based system's stakeholders - literature review

| Clusters | List nr. | Blockchain systems' stakeholders | Description | Authors |
|---|---|---|---|---|
| Cluster STK1 | SL1 | Systems Architects, Core Developers | Individuals and organisations who develop Blockchain systems including programmers, coders, software developers, system engineers etc. | Li, Greenwood, and Kassem (2019); Islam, Mäntymäki, and Turunen (2019) |
| | SL2 | Technology Providers, Hardware manufacters | Individuals and organisations who develop hardware, software, networking architecture for blockchain systems and those associated with enabling or interrelated technologies (e.g. IoT, sensors, drone technology). | Li, Greenwood, and Kassem (2019); Islam, Mäntymäki, and Turunen (2019) |
| | SL3 | Services providers | Companies involved in providing a technical service to organisations using Blockchain systems. | Li, Greenwood, and Kassem (2019) |
| Cluster STK2 | SL4 | Blockchain Council | Stakeholder groups of Blockchain systems tasked with approving changes to software, data in the ledger and ensuring technology and operations comply with regulations and who have the power over how Blockchain systems function in general. | Li, Greenwood, and Kassem (2019) |
| | SL5 | National Authorities / Policy Makers | State and local government authorities responsible for making policy, writing standards and setting regulations along with enforcing them. | Li, Greenwood, and Kassem (2019); Cagigas et al. (2021) |
| | SL6 | International Political Authorities | International groups working together to set international regulations for transactions that cross borders to promote international partnerships and to mitigate the possibility of fraud, corruption and other criminal activities. | Li, Greenwood, and Kassem (2019) |
| Cluster STK3 | SL7 | Individual Organizations , Exchange, Merchants | Individual organisations operating in a certain industry or domain. | Li, Greenwood, and Kassem (2019); Islam, Mäntymäki, and Turunen (2019) |
| | SL8 | Clients | Individuals or organisations, public and private, who commission projects with access to information on the ledger regarding their project. | Li, Greenwood, and Kassem (2019); |
| | SL9 | Investors | Individual investors, institutional investors. | Islam, Mäntymäki, and Turunen (2019) |
| | SL10 | Project Teams | Individuals across the supply chain who specifically form the project team who have access to the ledger and who have responsibility for producing information to the ledger or consuming information from the ledger. | Li, Greenwood, and Kassem (2019) |
| | SL11 | Individual users of the System | Individuals who use blockchain systems day-to-day either through performing transactions or by providing data to be uploaded to the ledger. | Li, Greenwood, and Kassem (2019) |
| | SL12 | Supply chain of a specific industry | Organisations that make up the supply chain for certain industry that are: concerned with technical elements of the system regarding tracking and updating ledgers; impacted upon regarding international politics and regulations where supply chains cross borders; have a responsibility to operate in a sustainable manner; and who must follow processes as set by industry standards and clients. | Li, Greenwood, and Kassem (2019) |
| | SL13 | Civil Servants | Public employees in charge of provision and/or regulation of the public services that are impacted by the use of blockchain systems implemented by the government. | Cagigas et al. (2021) |
| | SL14 | Citizens | Individuals who are the potencial recipients of the public services provided by blockchains systems implemented by the government. | Cagigas et al. (2021) |
| | SL15 | Miners | Individual miners, mining pools and mining organisations operating as nodes and running the peer-to-peer network. | Li, Greenwood, and Kassem (2019), Islam, Mäntymäki, and Turunen (2019) |
| Cluster STK4 | SL16 | Social groups | Groups of individuals with an interest in the impact of Blockckains systems at a societal level (e.g. regarding energy consumption, privacy, security, creation of a value-driven economy, ensuring societal needs are being met by technological solutions). | Li, Greenwood, and Kassem (2019) |
| | SL17 | Industry associations | Professional associations who represent the interests of individuals and organisations operating in a certain industry. | Li, Greenwood, and Kassem (2019) |
| | SL18 | Educational Institutions | Universities and other educational institutions conducting research and developing programmes to train and upskill people in relation to Blockchain systems. | Li, Greenwood, and Kassem (2019) |
| | SL19 | Communities of Practice | Groups of individual practitioners with an interest in a specific area of Blockchain (e.g. interoperability, privacy, speed). | Li, Greenwood, and Kassem (2019) |

### 2.3.3. What are the risks of the BBS?

Prewett et al. (2020) have discussed barriers and risks to the adoption of BBS. They argued that barriers are deficiencies that refrain companies and industries from adopting the BBS. Risks are related to vulnerabilities or circumstances not foreseen when dealing with BBS's adoption. Due to the clear differentiation between barriers and risks made by Prewett et al. (2020), when the mentioned barriers were considered risks in the papers reviewed, they were disregarded. Prewett et al. (2020) mentioned various barriers to the adoption of BBS: scalability; lack of integration with legacy systems; lack of coding standardization, and in consequence, lack of interoperability between systems; complexity of BBS applications; regulatory uncertainty; lack of knowledge, skills, and training.

The reviewed literature identified several risks that were very often presented into categories. However, the categories used vary per author. For example, according to White, King, and Holladay (2020), risks can be classified into technological risks, data security risks and third-party vendor risks. In Zetzsche et al. (2018), risks are classified into cyber, operational, and ledger transparency risks. Table 3 includes the risks identified in the literature review. The risks are classified into clusters. The clusters are displayed for visualization purposes only, as the literature reviewed has not used standard categories to present the risks. A complete literature review is included in Appendix 4.

One of the empirical research goals will be to identify BBS risks and verify whether the risks presented in the literature can also be confirmed empirically. Therefore, the same question will be subject to the empirical research: what are the risks of the BBS?

Table 3 - Risks of the blockchain-based systems - literature review

| Cluster nr | nr | Risks context | Authors |
|---|---|---|---|
| Cluster R1 | RL1 | Third party tracking (cookies) make possible the identification of personal details through the link between crypto wallets and web purchases made with crypto currencies. | Steven, Harry, Dillon, and Arvind (2018) |
| | RL2 | Each participant node might be subject to different compliance standards in different jurisdictions. | Prewett et al. (2020) |
| | RL3 | Potencial legal disputes. No consistent jurisdiction can be derived from location. Besides, the imutability of the system can clash with the data protection laws. | Cagigas et al. (2021) |
| | RL4 | Due to the transaparency of the data in the system, entities must consider and address their data privacy obligations. Additionally, data cannot be erased, due to immutability characteristic of the system. This context can infringe the data protection rules and clash with the law. | Zetzsche, Buckley, and Arner (2018); |
| | RL5 | Possible legal actions from the parties involved related to the outcome of the smart contract. | Nguyen, Chen, and Du (2020) ; |
| | RL6 | Due to the transaparency of the data in the system, it is possible to identify transactions and de-anonymize individuals. This context can infringe the data protection rules. | Cagigas et al. (2021) |
| | RL7 | Sensitive data ( trade volume or inventory levels) may facilitate market manipulation. It can lead to civil and criminal litigations. | Zetzsche, Buckley, and Arner (2018) |
| | RL8 | Private keys become the target of illicit activities | Zetzsche, Buckley, and Arner (2018) |

Table 3 - Risks of the blockchain-based systems - literature review (cont'd)

| Cluster nr | nr | Risks context | Authors |
|---|---|---|---|
| Cluster R2 | RL9 | Endpoint is where human and machine interface with the blockchain network. It is where data is captured, created and transmitted. | Prewett et al. (2020); |
| | RL10 | Risks of errors in the interface with the real world such as human interaction, communication with sensors and other devices. | Nguyen, Chen, and Du (2020) ; |
| | RL11 | Mismatch between the ledger and the reality outside the blockchain related to the errors on the data commuicated from the users to the system or the order of the recorded events in the ledger. | Nguyen, Chen, and Du (2020) ; |
| | RL12 | The use of blockchain system does not guarantee information quality, only the accuracy of the procedures within the systems. | Cagigas et al. (2021) |
| | RL13 | For the Blockchain as a service platforms ( used by consortium blockchian solutions), the instability of the blockchain platform is a risk. | Nguyen, Chen, and Du (2020); |
| | RL14 | Long term storage plan and the associated costs. | Prewett et al. (2020) |
| | RL15 | Digital assets could become irretrievable if private key is lost or stolen. | Prewett et al. (2020); |
| | RL16 | Governance of the systems are dependent on small group of developers, therefore security and reliability is at risk. Besides there is no accountability for underperformance or misconduct. | Zetzsche, Buckley, and Arner (2018); |
| | RL17 | A minority of experts dictates the rules of the systems and its governance. | Cagigas et al. (2021) |
| | RL18 | Considers the Risks of resistance to the implementation of the system and the risks of job reductions. | Cagigas et al. (2021) |
| | RL19 | In case of systems failure related to processing speed or security standards, there is no accountable person to be contacted. | Zetzsche, Buckley, and Arner (2018) |
| Cluster R3 | RL20 | All the architeture and design choices must be exhaustively tested before put into production. | Prewett et al. (2020) |
| | RL21 | Related to the physical and logical access made by private keys. Quantum computing represent risk to encryption algorithms. | Prewett et al. (2020) |
| | RL22 | Management and monitoring of public and private keys. Human element risk :input, retrieve and transfer of data is performed through established protocols and use of private keys. | White, King, and Holladay (2020) |
| | RL23 | Key leaking ( permissionless) or attack to the digital certificate (in permissioned blockchains). | Nguyen, Chen, and Du (2020); |
| | RL24 | Smart contracts will act according to the logic programmed not according to the intention. | Prewett et al. (2020) ; |
| | RL25 | Intended terms and condictions of the contract are misinterpreted in the transformation to smart contract. | Nguyen, Chen, and Du (2020); |
| | RL26 | Errors in execution due to misunderstanding or intentional fraudulent acts. | Nguyen, Chen, and Du (2020); |
| | RL27 | Risk of fraudulent programming of the smart contracts or exploitation of smart contract's weeknesses. | Nguyen, Chen, and Du (2020); |
| | RL28 | Errors or "bugs"will negativelly affect the system. Error will be spread over the whole system affecting many nodes and indviduals, or making the system vulnerable to attacks. | Zetzsche, Buckley, and Arner (2018) |
| | RL29 | Current cryptography algorithms in use are at risk with the development of quantum computing. | Fedorov, Kiktenko, and Lvovsky (2018) |
| | RL30 | Divergence of the ledger due to different consensus being applied or due to latency when differents version of the blocks are recorded in the ledger. | Nguyen, Chen, and Du (2020); |
| | RL31 | Advances in quantum computing and cryptography might cause an outdated technology infrastructure. | White, King, and Holladay (2020) |
| Cluster R4 | RL32 | Expose the contracting organisation due to vendor blockchain systems' weaknesses. | Prewett et al. (2020); |
| | RL33 | Weaknesses of third party system can bring risks to the contractor blockchain environment. | White, King, and Holladay (2020) |
| | RL34 | Rights per participants in the network can vary and are defined on the services level agreements(SLA) with the vendors. | Prewett et al. (2020) |
| | RL35 | Attacks on the blockchain ( ledger, nodes, smart contracts, cryptography) | Nguyen, Chen, and Du (2020) |
| | RL36 | This attack generates innacurate flow of information from the ICT systems to the blockchain. | Nguyen, Chen, and Du (2020) |
| | RL37 | Attack on the data system prior to storage on the blockchain will lead to inaccurate date being stored. | Zetzsche, Buckley, and Arner (2018) |
| | RL38 | cyberattacks due to poor coding, private key theft. | Cagigas et al. (2021) |
| | RL39 | Attack to multiple nodes, where the most transactions are concentrated which are relevant for the computation of the consensus. Some nodes are safer than others. | Zetzsche, Buckley, and Arner (2018) |
| | RL40 | This attack could delay the transactions and the transfers to the users. | Zetzsche, Buckley, and Arner (2018) |

## 2.4. Objective of the follow-up research

The literature reviews' results have indicated the definition of BBS, identified stakeholders, and risks of BBS. However, further research is needed to confirm whether the stakeholders and risks found in the literature are confirmed empirically. Therefore, the empirical research has the goal to answer the following questions:

**RQ1: What are the stakeholders in a blockchain-based system?**
**RQ2: What are the risks of a blockchain-based system?**

Additionally, attempting to identify an intersection between risks and stakeholders, articles that have identified BBS stakeholders (in section 2.3.2) have also been screened in the search for risks. As only one article (Cagigas et al., 2021) has presented risks associated to stakeholders (public domain), it is necessary to conduct empirical research with the objective to identify risks associated to stakeholders and, in this way, contribute to answering the main research question:

**RQ3: What are the risks to the stakeholders involved in a blockchain-based system?**

The empirical research seeks to provide answers that will enable the set-up of a framework associating risks to the stakeholders. The framework aims to serve as a guideline to practitioners in a future BBS implementation process and contribute to the research community by adding empirical results to the BBS research domain.

# 3. Methodology

This chapter provides details of the empirical research design, strategy and source of information to be used in the research. It also includes a description of the operationalization, data collection methods and data analysis techniques. Finally, this chapter discusses the provisions to reinforce research quality and meet internal and external validity, reliability, and ethics requirements.

## 3.1. Conceptual design: selection of the research method

The main goal of the empirical research is to build a framework associating risks for the stakeholders in a BBS to answer the main research question. Additionally, the empirical research aims to verify whether the literature review results can be empirically validated.

The empirical research is designed in order to answer the following questions:

RQ1 - What are the stakeholders in a BBS?
RQ2 - What are the risks of a BBS?
RQ3 - What are the risks to the stakeholders of a BBS?"

The "what's" in questions 1 and 2 present characteristics of a descriptive research, which focuses on acquiring a profile of stakeholders and risks. The "what" concerning the research question 3 presents characteristics of an exploratory research, which aims to present associations between RQ1 and RQ2 to answer RQ3, the main research question.

Different sources of information can be used to perform empirical research: people; media; observation and/or measurement of real situations; documents; literature. Verschuren and Doorewaard (2007) highlight that people might be the most important source of information since they can provide information that can be collected in a short amount of time. Considering that this research is interested in people's (stakeholders) perceptions of risks, "people" is chosen as the primary source of information. Evaluation regarding other sources types is included in Appendix 5.

Research can be qualitative or quantitative. Quantitative research is based on statistical analysis, while qualitative research is based on non-numerical information. The nature of the research questions indicates that this is qualitative research.

Saunders, Lewis, and Thornhill (2019) described different strategies for qualitative research. Few of them are considered acceptable for this Master Research: Survey, Case study, Structured Literature Review and Grounded theory method. The Grounded theory method option is excluded due to its complexity and time available for this master research. The structured literature review has been performed in chapter 2, and it demonstrated to be insufficient in answering the main research question. Therefore, this strategy is disregarded. A case study would focus the research on the analysis of stakeholders and risks within the context of a company's borders, which would bring limitations to the study in relation to the context of the stakeholders within a company. A survey is a strategy that allows collecting information from participants who belong to different environments and therefore has been the method selected to collect the data for the empirical research.

In order to collect the data on a qualitative survey, it can be chosen between a longitudinal survey or a cross-sectional survey. The former considers data collection over time. The latter collects data in a pre-defined moment. Considering that this research has a strict timeframe, a cross-sectional survey is chosen as suitable.

## 3.2. Technical design: elaboration of the method

The elaboration of the method described in this section explains what data is needed, how it will be gathered and analyzed to answer all three research questions.

### 3.2.1. Data collection method and technique

The use of people as the primary source of information leads to two methods of data collection: interrogation or observation (Verschuren & Doorewaard, 2007). The research question's nature indicates that observation does not apply to this research. In the interrogation method, the researcher can stimulate the person to provide information that is relevant to the research. Therefore, the interrogation method will be used.

Interrogation relates to two techniques: questionnaires or interviews. Questionnaires are not flexible, composed of closed questions, with a pre-defined order and where neither the researcher nor the person providing information can interfere with additional questions nor further explanation, known as structured interrogation. It is used to test hypotheses in quantitative research, therefore not applicable to this research. The interview technique allows the researcher to lead the data collection with pre-defined themes and questions, however, having the possibility to interact with the interviewee whenever necessary, considered a semi-structured form of interrogation. As this research is interested in identifying stakeholders, risks and their associations based on personal insights, a semi-structured interview is chosen as the technique for data collection.

### 3.2.2. Development of interview questions

General questions will be included at the beginning of the interview to provide context for the interviewee's background and experiences. The leading questions will include the empirical research questions: what are the stakeholders of the BBS, what are the risks of the BBS and what are the risks to the stakeholders in a BBS. Additional questions will be intercalated with the leading questions to induce the interviewee to reflect on the answers provided. In a semi-structured interview, the researcher may include further questions with the objective to clarify any topic during the interview, as needed. The interview questions, including details of the motivations per question, are disclosed in Appendix 6.

### 3.2.3. Operationalization

The operationalization described below, related to the information that will be collected during the interviews, is applied to all three research questions.

**Step 1 - Selection and invitation of participants**

In order to identify professionals that meet the participant's profile (Appendix 7), professionals with different backgrounds and active in a variety of business domains will be randomly selected, using the researcher's private network by direct contact or using the professional network LinkedIn. The first contact will be made per email (Appendix 8), explaining the research subject, the profile required, and the request to participate in the interview. After a positive response, the ZOOM meeting tool will be used to send the invitation with the proposed dates for the interview. Considering the time available for this research, the expectation is to interview a total ranging from five up to six participants.

**Step 2- Test interview**

A test interview will be performed with one of the participants to verify if the interview questions (Appendix 6) are straightforward and whether the time scheduled is sufficient to answer all questions. Besides, the test interview will assist in identifying any other constraints during the interview. The results from the test interview will be used to adjust the interview questions, if necessary. If no adjustment is needed after the test interview, the same interview questions will be used in the following interviews.

**Step 3 - Participant's interview protocol**

In order to provide the necessary information related to the research topics, a participants' interview protocol (Appendix 9) will be used to guide the interview. Further details as the duration of the interview, permission for recording, and data privacy provisions will also be disclaimed to the participants. The participants' interview protocol will be sent in advance by email.

**Step 4 - Data collection - interviews**

Due to COVID restrictions, the interviews will be conducted online using the meeting tool ZOOM. The semi-structured interviews will be conducted according to the questions outlined in appendix 6 and will follow the step-by-step interview procedures (Appendix 10). The individual interviews will take approximately 1 hour. Each researcher from the team will perform five to six interviews and will transcribe the interview records. As the research team comprises five researchers, a total ranging from 20 up to 25 interviews records is expected to be available for the group data analysis.

## 3.3. Data analysis

The interview transcripts will be coded and shared among the researchers using the "in vivo coding standard form" (Appendix 13). The standard form is developed jointly with the researcher's team and contains interview topics (Introduction, Stakeholder, Risks, Risks to Stakeholders) and focuses on coding only relevant information to the research questions. The form seeks to create standardization among researchers during the data analysis process, considering that the conduction of semi-structured interviews may vary from interview to interview, according to the need for additional clarifying questions.

The stakeholders and risks identified by the empirical research related to RQ1 and RQ2 will be categorized using the template analysis technique described in Saunders et al. (2019). By the creation of the template, three types of coding will be used: codes derived from the literature (a priori codes); codes named by participants during the empirical research (in vivo codes); and codes suggested by the researcher, derived from the data, used in case the other coding approaches do not apply. Saunders et al. (2019) suggest beginning with "a priori" codes and supplementing it with the "in vivo" codes identified from the data. A complete data analysis protocol is included in Appendix 12.

One criticism of the template analysis is that the researcher "may become too focused on applying the template to the data, rather than using the data to develop the template" (King and Brookes, 2017, in Saunders et al., 2019, p. 664). Therefore, to avoid individual bias, the decision is made to perform a group data analysis and develop the template jointly with the research team.

The RQ3 is answered by indicating all the risks associated with the stakeholders unveiled during the interviews. The results will be displayed in a matrix as a technique for data display (Miles et al., 2014, in Saunders et al., 2019, p. 690).

## 3.4. Reflection w.r.t. validity, reliability, and ethical aspects

This section includes information on the provisions taken by the researcher in complying with research quality, based on quality criteria's guidelines in qualitative research described in Shenton (2004).

**Internal Validity**

As argued by Shenton (2004), internal validity is the degree of credibility in qualitative research. Some measures are taken to reinforce the internal validity.

i. The interview protocol is discussed at the beginning of the interview to certify that all topics are well understood.
ii. A test interview is performed to verify the comprehensibility of the interview questions.
iii. The data analysis is performed jointly with the research group to avoid individual bias.

**External Validity**

Shenton (2004) points out that qualitative research is in general unable to make assumptions related to generalization, whether the findings can be applied to a broader group, considering that findings from qualitative research are related to a smaller sample than generally used by quantitative research. Moreover, the findings are specific to a particular environment or individuals, therefore not possible to demonstrate generalizability. The guidelines from Shenton (2004) were followed, seeking to meet this quality criteria. Therefore, the reader will find a detailed description of the research design, the operationalization process, data collection and analysis to provide other researchers with sufficient information that may allow comparisons with future studies utilizing the current results in a broader population.

**Reliability**

Reliability refers to the dependability of the research in case it would have to be repeated. For this quality criteria, the reader will find a detailed description of the research design, the operationalization process, data collection, data analysis, and a reflective appraisal of the research, as advised by Shenton (2004).

**Ethical Aspects**

Following the ethical principles included in the guidelines of the master research, the researcher has taken the following actions:

i. Requested formal consent from participants to record the interviews.
ii. Informed the participants that they may withdraw from the research at any time.
iii. Informed the participants that the data collected will be used for academic purposes only.
iv. Informed the participants that the data collected will be anonymized, respecting data privacy guidelines.
v. Informed the participants that during the research process, the interview video records will be maintained, separated from the research files, and deleted once the deadline for keeping records is expired.

# 4. Results

The initial objectives of the empirical research are to confirm whether the stakeholders and risks found in the literature review are confirmed and whether any additional stakeholders and risks are identified. The first two empirical research questions are:

**RQ1: What are the stakeholders in a blockchain-based system?**
**RQ2: What are the risks of a blockchain-based system?**

The third and main research question is:

**RQ3: What are the risks to the stakeholders of a BBS?**

The results of the empirical research are presented in the following sections.

## 4.1. Participant's selection

Participants for the interviews were selected and contacted via the researcher's private network. Due to the lack of personal contacts with experience in BBS, the personal network has been approached randomly requesting for indication of someone with the participant's profile (Appendix 7). Once potential participants were identified, they were contacted by email (Appendix 8) and requested to participate in the interview. Once the participation was confirmed, they received a ZOOM invitation for the interview.

Provisioning for unexpected issues, a total of 10 people were invited to the interviews. After the participation confirmation, there was one cancelation due to sickness and two other people that did not accept the ZOOM invitation for the interview, despite reminders. The background information of the interviewees is included in table 4.

Table 4 - Interviewees details

| REF. | Country | Function | Industry | Years Blockchain experience | Interview Date |
|---|---|---|---|---|---|
| TEST | Brazil | Blockchain Services LATAM Leader | Technology services | 5 | 13-Sep |
| DM01 | England | Founder blockchain analytics service provider | Technology services | 6 | 14-Sep |
| DM02 | Netherlands | Program Manager Telecom | Energy Infrastructure | 3 | 20-Sep |
| DM03 | Finland | Solidity developer | Independent consultant | 5 | 24-Sep |
| DM04 | Netherlands | Business Analyst | Energy Infrastructure | 5 | 27-Sep |
| DM05 | Netherlands | Innovation Project manager | Energy Infrastructure | 3 | 28-Sep |
| DM06 | Brazil | Senior Manager Blockchain Practice | Professional services | 4 | 28-Sep |

## 4.2. Test interview

A test interview was performed to evaluate whether the final questions were clear to the participant, identify any possible issues with the questions and verify the feasibility of the scheduled one-hour duration for the interview. The participant received the interview protocol (Appendix 9) in advance, and the test interview was conducted according to the interview procedures (Appendix 10). The test interview is successfully performed and completed within the time scheduled. No issues were identified. Details of the test interview are included in Appendix 11.

## 4.3. Data collection semi-structured interviews

In advance, all the participants received the interview protocol (Appendix 9) containing the interview questions and guidelines for the interviews. The interviews were conducted according to the interview procedures (Appendix 10). A total of six semi-structured interviews were performed.

The six interviews performed were recorded and transcribed by the author of this dissertation. The six interviews transcripts files are included in Attachment 1 . (Another ten interviews were performed and transcribed by other team members). The expected total of 20 to 25 interviews for the research as a group is not achieved due to the reduction of the research team, which started with five members, and at this phase, only three researchers were able to contribute with interviews information to the data analysis, described in the next section.

## 4.4. Results Data analysis

The data analysis has followed the data analysis protocol included in Appendix 12.

The stakeholders and risks identified either in the literature review, described in chapter 2, and identified during the empirical research, included in the in vivo coding forms (Appendix 13.1 to 13.6), have been used for the creation of the stakeholders and risks templates, which provided answers to RQ1 and RQ2, presented in sections 4.4.1 and 4.4.2, respectively.

The answer to the RQ3 is presented in a matrix, which shows the identified associations between stakeholders and risks. The matrix has compiled the data from the in vivo coding forms (Appendix 13.1 to 13.6). Due to its size, the complete matrix file is included in Attachment 2. A condensed version, including stakeholders associated per risks categories, is disclosed in the results in section 4.4.3.

**Templates creation - general comments on the process execution**

The creation of the initial template using “a priori” codes has consumed 13.5 hours of group meetings (One physical kick-off meeting with the duration of 3h and seven additional online group meetings of 1.5 hours each). The preparation of the final template, which used the information from the in vivo codes, has consumed 8 hours, split into five group meetings. In total, 21,5 hours of group analysis were necessary to achieve the final version of the two templates created (stakeholders and risks). The time consumed differs from the 12 hours expected for this process, as initially described in the data analysis protocol.

Initially, four researchers (the fifth researcher was no longer participating in the group) have used the results from their literature review to contribute to the first phase of the template creation (“a priori” coding). The stakeholders and risks identified in the literature review differ among the research group members since each researcher has independently performed a literature review according to different search queries.

The final phase of the template analysis uses the results from empirical research. In this phase, the interview transcripts were coded ("in vivo" coding) and shared among the researchers. Only three researchers contributed to this process since the fourth researcher had not performed any interviews until the data analysis had started.

The templates provide categories and sub-categories for the stakeholders and risks that comprise the answers for RQ1 and RQ2. The print screens of the final templates created are disclosed in Appendix 16, presented in Dutch (the common language of the research group). All the categories, sub-categories, and definitions from both templates have been translated into English and presented in Appendices 14 and 15.

During the template creation, the research group followed the procedures described on the data analysis protocol (Appendix 12) and has created categories/sub-categories or coding classifications only when an agreement was reached within the research team. Items that did not fit the existent categories remained in the "uncategorized items" until the creation of a new category or sub-category. Debatable items were postponed to the following sections or discussed at the end of the section when no other items were uncategorized. During the process, the researchers participated actively in the discussions as a group.

During the process of templates creation, there have been three deviations from the data analysis protocol (Appendix 12), as described below.

In step 5.8, part of the "in vivo" data analysis, data reduction has not been performed. The group considered that all the individual stakeholders and risks identified would be needed to create the matrix with the association between risks and stakeholders when answering RQ3. For this reason, there has not been any data reduction. All risks and stakeholders mentioned during the empirical research were considered for the results.

Due to time constraints, the group effort is finalized after completing the templates. The last two steps from the data analysis protocol (5.11 and 5.12) were performed individually and followed the process described below:

In step 5.11, the results of the categorizations were included in two excel tables (stakeholders and risks). All items were compared with the literature lists results presented in chapter 2. The items equivalent to existing literature's names and definitions were not replaced. Instead, the identified equivalent literature is informed in an extra column, keeping the empirical records intact.

In step 5.12, the matrix is created individually, and each researcher has built the matrix based on the results of their own interviews only. The results from this step provided answers to RQ3, discussed in section 4.4.3.

### 4.4.1. RQ1 - What are the stakeholders in a blockchain-based system?

A stakeholders' template is developed (Appendix 14) to present the categorization of the stakeholders' types.

At the start of the process for template development, the literature results were considered and served as the basis for creating the initial categories: technical stakeholders, political stakeholders, process stakeholders and social groups, which derived from the dimensions described in Li et al. (2019). As not all stakeholders from the literature list could be categorized within the initial categories, the "investors" category was created. Upon a new category creation, its definition was drafted. The definition of a category or a sub-category guided a consistent classification of items. Subsequently, the stakeholders were categorized.

The process stakeholders were initially split into the sub-categories, active and passive. However, after discussions, the group has agreed that there was not enough information available to classify the stakeholders according to passive and active. Therefore, these sub-categories were canceled, and all the process stakeholders returned to the main category process stakeholders.

As part of the iterative process related to the template analysis technique, all the stakeholders per category were iteratively reviewed as described in the data analysis protocol (Appendix 12). The review permitted the identification of clusters, which followed the creation of the sub-categories and their definitions. For instance, the category of technical stakeholders is expanded with two sub-categories: vendors and developers. Subsequently, the process stakeholder's category is re-analyzed, and three sub-categories were created: individual organizations, end-users, and node runners. The categories political, social, and investors remained without subcategories in this phase of the template creation.

Afterward, the stakeholders' template is further developed in the next phase ("in vivo"). The codes derived from the in vivo coding forms (Appendix 13.1 to 13.6) were added and categorized. In this phase of the template creation, additional categories and sub-categories were needed to classify new stakeholders identified during the empirical research that did not meet the definitions of the existent categories. For instance, the main category "others" was created to classify the stakeholders for which no clear role definitions were given during the interviews. The technical stakeholder category is expanded with one additional sub-category: "facilitators." Following the same procedure, the process stakeholder's category is also expanded with the sub-category "project managers," and in the category investors, two sub-categories were created: "internal investors" and "external investors."

The empirical research has identified 39 stakeholders, disclosed in Table 5. The stakeholders have been categorized simultaneously with the template created (Appendix 14). The last column of Table 5 informs whether the stakeholder is newly identified by the empirical research or previously disclosed in the literature review. The equivalent number from the literature review list (table 2 chapter 2) is included for traceability. There has been no stakeholder identified for the sub-categories S3.3 Node runners, S4.1 External investors, nor in category S5 Social groups; hence these sub-categories are not displayed, even though they are part of the final template created. Banks and financial institutions have been mentioned as stakeholders. However, as their role has not been clarified during the interviews, they were included in the category S6 "other."

Table 5 - Identified stakeholders from empirical research

| Categories and sub-categories | | Empirical results: Stakeholders | Empirical results: Stakeholders' roles | interview source | Identified literature or new stakeholder? |
|---|---|---|---|---|---|
| S1. Technical stakeholders | S1.1 Developers | Developers | Write the code on the contract. | DM03 | SL1. Systems Architects, Core Developers |
| | | Software Architects, developers | Architects and developers design/build together technical requirement of the system. | DM06 | |
| | S1.2 Vendors | Energy Web foundation | Developers team are building company's application on the top on the EWF's blockchain. | DM04 | SL2. Technology Providers, Hardware manufacters |
| | | Device Manufacturers | Manufactures the device that will be onboarded on the blockchain. | DM04 | |
| | | Hardware supplier | Provides the devices that gather all data, there is no direct interaction with the blockchain. | DM05 | |
| | | Technology Services Providers | Third parties that can join depending on what capability they can add, for example cloud services, or a part of the BBS as a service. | DM06 | |
| | | IT software provider | Builds the software platform and the forecast systems and algorithms. | DM05 | SL3. Services providers |
| | S1.3 Facilitators | Technical teams | The technical teams are related to the normal IT requirements like connection , security requirements, etc. | DM06 | new |
| | | Administrator | IT support role that manages the contract once it is deployed ( puts the contract on hold for example in case there is a bug, or funds are stolen, or investigates any other error). | DM03 | new |
| | | Internal installers (Infrastructure ) | Deals with the installation process of the physical devices that produce information (scanned QR codes) to the blockchain . Make sure that the asset is properly identified and authorized. | DM04 | new |
| | | External installers (Infrastructure ) | External parties contracted to execute the same as the internal installers. | DM04 | new |
| | | Internal IT department | Analyze the enterprise architecture to evaluate the future scalability of the blockchain solution within the company enterprise architecture. | DM05 | new |
| S2. Political stakeholders | | Regulators | Evaluate if the blockchain being used is meeting the rules established by the privacy laws. | DM02 | SL5. National Authorities / Policy Makers |
| | | Municipalities | Interested in how the blockchain project is contributing to their sustainability goals and targets. | DM05 | |
| | | Regulatory ( intern department) | Verify blockchain compliance with regulatory requirements. | DM05 | new |
| S3. Process stakeholders | S3.1 Individual Organizations | Energy producer companies | Producers of energy - interested in the balance of the energy grid. | DM02 | SL12. Supply chain of a specific industry |
| | | National Grid energy distributors | Deliver energy - interested in the balance of the energy grid. | DM02 | |
| | | DSO - Grid management | Interested in maintaining a balanced energy grid. The DSO controls information to make sure the demand is attended and the grid is balanced. | DM02 | |
| | | Exchanges | See the contract as a commodity, they are a market place provider; they do not interact with the contract. | DM03 | SL7. Individual Organizations , Exchange, Merchants |

Table 5 - Identified stakeholders from empirical research (cont'd)

| | | Empirical results | | | |
|---|---|---|---|---|---|
| Categories and sub-categories | | Stakeholders | Stakeholders' roles | interview source | Identified literature or new stakeholder? |
| S3. Process stakeholders | S3.2 End users | Trading Operators | Indirectly users of the blockchain information for trading purposes. Receive the information from the Blockchain Analytics services provider. | DM01 | SL11.Individual users of the System |
| | | Asset Managers (of investment funds) | Indirectly users of the blockchain information for trading purposes. Receive the information from the Blockchain Analytics services provider. | | |
| | | Blockchain Analytics service provider | Uses the information from BBS to provide blockchain analytics services to clients. | | |
| | | Researchers (intern) | Working at the service analytics providers to provide information to the clients. | | |
| | | Traders (retail) | Use information through the exchanges. | | |
| | | Consumers (of energy P2P)/ Residents | Participants of the smart contracts in order to consume energy in local communities ( peer-to-peer energy exchange in local communities - microgrids). | DM02 / DM05 | |
| | | Prosumers | Households (small producers) who produce energy and participate in the smart contracts delivering the energy from solar panels to the local communities. | DM02 | |
| | | End user smart contract | Customers using the smart contract . | DM03 | |
| | | Consumers (owner of an external asset) | Uses the assets that are registered in the system (e.g. electric vehicle). Reporting this vehicle in the blockchain is important for the capacity planning of the energy grid. | DM04 | |
| | | Telecom department | They set up use cases of the assets (routers ) that should be onboarded. Analyses possibilities of onboarding communication devices on the blockchain, related to the improvement of security in communication. | DM04 / DM05 | SL10. Project teams |
| | | Asset management department | Functional owner of the assets, deliver the business rules for the blockchain. Main users of the systems since they are responsible for the management of the assets onboarded in the system ( Planning life cycle of the assets and new purchases). | | |
| | | Supply chain | Part of the ecosystem that will use the BBS. They provide the project team with their view of the processes to be used in the system design , that should attend the business needs of all participants. | DM06 | SL12. Supply chain of a specific industry |
| | | Cooperatives | Part of the ecosystem that will use the BBS. They provide the project team with their view of the processes to be used in the system design , that should attend the business needs of all participants. | | |
| | S3.4 Project managers | Project Development Team | Interact with the various stakeholders on behalf of the interests of the company. | DM02 | new |
| | | Business management of the project | Project management (e.g. CTO). | DM03 | new |
| | | Innovation department / Project management | Leads the blockchain project, responsible for the idea, start of the project and also the first design of the logic for the blockchain project. | DM04/ DM05 | new |
| | | Business Project Teams | Build the business design of the project, keep the agile development, agree on definitions for the smart contracts, manage project priorities etc. Project unifications within the participating stakeholder. | DM06 | new |

Table 5 - Identified stakeholders from empirical research (cont'd)

| | | Empirical results | | | |
|---|---|---|---|---|---|
| Categories and sub-categories | | Stakeholders | Stakeholders' roles | interview source | Identified literature or new stakeholder? |
| S4. Investors | S4.2 Internal investors | Deployer of the contract | Commissions ( or contracts) and provide funding for the creation of the smart contract. | DM03 | SL8.Clients |
| | | Client Management Team | Management team that contracts and funds the project. They define the business processes, business rules, and provide the characteristics of the asset that will be included in the BBS. Final responsibility for onboarding all the necessary stakeholders to the BBS ecosystem. | DM06 | |
| S6. Other | | Banks and financial institutions (*) | Banks and financial institutions have been mentioned as stakeholders, however their role in the system has not been discussed, therefore it is not clear what their role is in the BBS. Therefore placed in the category others. | DM06 | N/A |

### 4.4.2. RQ2 - What are the risks of a blockchain-based system?

The risks template is developed (Appendix 15) and utilized to display the risks into categories. Following a continuous and iterative process of analysis, classification, and reclassification, as described in the data analysis protocol (Appendix 12), the "a priori" and "in vivo" phases of the process were followed in the development of the risks template.

At the start of the process for the creation of the initial template (based on the "a priori" codes), risks categories identified in the literature were used: technical risks (Li et al., 2019), cyber risks, and legal risk (Zetzsche et al., 2018). All risks that fit into these initial categories were classified. Clusters were formed with the items that remain uncategorized in order to identify similarities. The items classified under "cyber risks" were compared with the uncategorized risks in further analysis. Subsequently, a discussion was raised with the argument that different types of criminal risks should be categorized together, and for this reason, the "cyber risks" category was considered too narrow, not permitting the inclusion of the fraud risks identified. This discussion caused the change in the category name from "cyber risks" to "criminal use risks," and two sub-categories were created: attack risks and fraud risks. Subsequently, the analysis of the clusters in the technical risks category also indicated the need for further classification. Therefore, three sub-categories were included in the technical risks category: coding, infrastructure, and governance risks. All the remaining uncategorized risks were further analyzed, and three new categories were created: Privacy risks, human risks, and financial risks.

The risk template is further developed in the "in vivo" phase of the process. This phase categorized the risks identified during the empirical research. The category "business case risks" was initially added to the template. After further analysis within this category, two sub-categories were created: Strategic risks and Lack of adherence to the system risks. Finally, the category economic risks and its definition was added to the template. At the end of the "in vivo" phase, the final template created included the following categories: Criminal use risks (split into sub-categories attack risks and fraud risks); technical risks (split into sub-categories coding, infrastructure, and governance); Privacy risks, legal risks, human risks, financial risks, business case risks (split into sub-categories strategic risks and lack of adherence to the system risks") and economic risks.

The empirical research has identified 33 risks, categorized simultaneously with the template developed (Appendix 15). The results are disclosed in Table 6, which shows in the last column if a risk is newly identified by the empirical research or previously disclosed in the literature review. The equivalent number from the literature review list (table 3 chapter 2) is included for traceability. No risk has been identified for the sub-category R1.1 (attack risks) or category R8 (economic risks). Hence

these categories are not displayed in the results even though they are part of the final template created.

Table 6 - Identified risks from empirical research

| | | Empirical results | | | |
|---|---|---|---|---|---|
| Categories and sub-categories | | Risks | Risks descriptions | interview source | Identified literature or new risk? |
| R1. Criminal use risks | R1.2 Fraud risks | R1.2.1 Risk of malicious installer | The risk that an external party is using the system in a malicious way. | DM04 | RL37.Tampering data prior to storage |
| | | R1.2.2. Risk of malicious manufacturers | The risk that an external party is using the system in a malicious way. | DM04 | |
| | | R1.2.3 IoT security breaches | The risks that the IoT devices can be manipulated without being noticed and therefore their data will be manipulated. | DM05 | |
| R2. Technical risks | R2.1 Coding risks | R2.1.1 Security code risks (monetary value loss) | Risk that the value locked in the contract can be stolen by unauthorized people. | DM03 | SL24. Smart contract risks |
| | | R2.1.2 Bugs risks | The risk that a mistake is inserted in the code and that is not identified on time during the tests. | DM03 | SL20. Architecture and design risks |
| | | R2.1.3 Security risks | Evaluation of levels of access to the system established in the SLA (service level agreement), code security in the smart contracts, possible information leak. | DM06 | RL34. Contractual risks / RL24. Smart contract risks |
| | R2.2 Infrastructure risks | R2.2.1 slow & cumbersome (scalability) | System is very slow, being this a big risk for adoption. | DM01 | • |
| | | R2.2.2 Uncertainty transactions confirmations | There is a risk that the transaction will not complete or will take long to confirm its completion. | DM01 | NEW |
| | | R2.2.3 Project management risk (time and functionalities) | The risk that the project will not be finalized on time or includes all the functionalities required. | DM03 | NEW |
| | | R2.2.4 Unavailability risks | The risk of the unavailability of the system (caused by bugs or other misfunctions) , since the system is not internally controlled, but controlled by the blockchain provider. | DM04 | RL13. Instabilities of the support platform |
| | | R2.2.5 Risk of incorrect assets register | The risks of not correctly identify the onboarding assets, due to the still use of different systems , causing discrepancies. | DM04 | RL12. Not inherently trustworthy |
| | | R2.2.6 Scalability risk | The risks that the solutions will not be scalable. | DM05 | • |
| | | R2.2.7 Standardization risk | The risks that the various blockchain pilots projects are not operating together. | DM05 | • |
| | | R2.2.8 Continuity risks | The risk that the blockchain service provider stops its activities. It is an external party and the company has no control about it. | DM05 | NEW |
| | | R2.2.9 Project technical viability risks | Risks of the project not being technically viable. This risk is present when after first preliminary analysis of the project proposal from the business stakeholders, the technical teams judge the viability of the project. | DM06 | NEW |
| | | R2.2.10 Integration with existing systems risks | Risks of the various systems not being interconnected with the BBS, creating silos that may create operational issues. | DM06 | • |
| | R2.3 Governance | R2.3.1 Transaction costs risks | Risk of increased transaction costs when considered a better performance request from the system. | DM06 | NEW |
| R3. Privacy r | | R3.2 Privacy legislation risk | The information disclosed on the blockchain should meet the restrictions of the privacy regulations, which can be differently interpreted by National regulators and European Regulators. | DM02 | RL2. Compliance risks |
| | | R3.3 Data privacy risks | Risks of exposure of the business data. | DM06 | RL6. Risk of reidentification |
| R4. Legal risks | | R4.1 Regulatory risk | Uncertainties about regulations. | DM01 | • |
| | | R4.2 Legal/compliance risk | Risks in relation to laws and regulatory requirements. | DM06 | RL2. Compliance risks |

Table 6 - Identified risks from empirical research (cont'd)

| | | Empirical results | | | |
|---|---|---|---|---|---|
| Categories and sub-categories | | Risks | Risks descriptions | interview source | Identified literature or new risk? |
| R5. Human risks | | R5.1 Complexity risks | The risks that a lot of people will not understand what the system does and how it should work. | DM04 | * |
| | | R5.2 Lack of business research /Project visualization risks | The risk of not compiling a complete and in deep understanding of the business requirements, technical design and assets involved when approving the final design for the project . The risk of not connecting all the dots related to the project. | DM06 | NEW |
| R6. Financial risks | | R6.1 Costs | Transaction fees can become expensive. | DM01 | NEW |
| | | R6.2 Financial Risks (ROI) | Risk of the initial investment will not produce the expected impact/return. | DM06 | NEW |
| R7. Business case risks | R7.1 Strategic risks | R7.1.1 Few barriers to entry (competitors) | Because it is based on a public information from the blockchain and anyone can start doing the same. | DM01 | NEW |
| | | R7.1.2 Market product fit risks | Will the final designed product by the smart contract have the acceptation in the market? | DM03 | NEW |
| | | R7.1.3 Business case risk | The risk that the blockchain project does not produce any monetary value advantage. | DM05 | NEW |
| | | R7.1.4 Business continuity risks | Risks that the continuity of the company and its business may be affected. | DM06 | NEW |
| | R7.2 Lack of adherence to the system risks | R7.2.1 Lack of adherence to the system risks | Risk that the participants of the ecosystem will not see the benefits of adherence to the system. | DM06 | NEW |
| | | R7.2.2 Reputational/brand risks | Risks of possible effects to the brand in case any failure occurs with the project that effect the whole ecosystem. Risks of damage to the brand. | DM01 / DM06 | NEW |
| | | R7.2.3 Systemic risks (throughput-time, availability, information leak) | The risk of spreading various risks along to the various companies participating in the ecosystem. | DM06 | NEW |

The results marked with an " * " in the last column of Table 6 were risks identified in the view of the interviewed stakeholders. The literature reviewed does not recognize them as risks and instead considers them barriers to BBS adoption. Details of the differentiation between risks and the barriers to adoption of BBS can be found in Prewett et al. (2020), as discussed in chapter 2, section 2.3.3.

### 4.4.3. RQ3 - What are the risks to the stakeholders in a blockchain-based system?

The main research question is answered by compiling the risks to the stakeholders unveiled during the empirical research. Due to its size, the final matrix is attached instead of included in the appendix. The final matrix lists all the risks associated with all the stakeholders identified. There were 10 risks identified in the infrastructure category, which is the category that has the highest number of stakeholders related to it (22 stakeholders). The second and third most associated risk categories were privacy risks (16 stakeholders) and strategic risks (15 stakeholders). Table 7 presents a condensed version including the associations between stakeholders and the risks categories.

Table 7 - Risks to the stakeholders

| Categories and sub-categories | | Stakeholders | R1. Criminal use risks | R2. Technical risks | | | R3. Privacy risks | R4. Legal risks | R5. Human risks | R6. Financial risks | R7. Business case risks | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | R1.2 Fraud risks | R2.1 Coding risks | R2.2 Infrastructure risks | R2.3 Governance risks | | | | | R7.1 Strategic risks | R7.2 Lack of adherence to the system risks |
| S1. Technical stakeholders | S1.1 Developers | Developers | | x | x | | | | | | | |
| | | Software Architects, developers | | x | x | x | x | | | | x | x |
| | S1.2 Vendors | Energy Web foundation | | | x | | | | | | | |
| | | Device Manufacturers | | | x | | | | x | | | |
| | | Hardware supplier | x | | x | | | | | | x | |
| | | Technology Services Providers | | x | x | | x | | | | x | x |
| | | IT software provider | x | | x | | | | | | x | |
| | S1.3 Facilitators | Technical teams | | x | x | x | x | | | | x | x |
| | | Administrator | | x | | | | | | | | |
| | | Internal installers (Infrastructure ) | x | | x | | | | x | | | |
| | | External installers (Infrastructure ) | | | x | | | | x | | | |
| | | Internal IT department | x | | x | | | | | | | |
| S2. Political stakeholders | | Regulators | | | | | x | | | | | |
| | | Municipalities | x | | x | | | | | | x | |
| | | Regulatory ( intern department) | | | x | | | | | | x | |
| S3. Process stakeholders | S3.1 Individual Organizations | Energy producer companies | | | | | x | | | | | |
| | | National Grid energy distributors | | | | | x | | | | | |
| | | DSO - Grid management | | | | | x | | | | | |
| | | Exchanges | | x | | | | | | | | |
| | S3.2 End users | Trading Operators | | | x | | x | | | x | | |
| | | Asset Managers (of investment funds) | | | | | x | x | | | | x |
| | | Blockchain Analytics service provider | | | | | | | | | x | |
| | | Researchers (intern) | | | | | | | | x | x | |
| | | Traders (retail) | | | x | | | | | x | | |
| | | Consumers (of energy P2P)/ Residents | | | | | x | | | | x | |
| | | Prosumers | | | | | x | | | | | |
| | | End user smart contract | | x | | | | | | | x | |
| | | Consumers (owner of an external asset) | | | x | | | | x | | | |
| | | Telecom department | x | | x | | | | x | | | |
| | | Asset management department | x | | x | | | | x | | | |
| | | Supply chain | | | | | x | | | x | | x |
| | | Cooperatives | | | | | x | | | x | | x |
| | S3.4 Project managers | Project Development Team | | | | | | | | | | |
| | | Business management of the project | | | x | | | | | | | |
| | | Innovation department / Project management | x | | x | | | | x | | x | |
| | | Business Project Teams | | | x | x | x | x | x | x | x | x |
| | S4.2 Internal investors | Deployer of the contract | | | x | | | | | | x | |
| | | Client Management Team | | | | x | x | x | x | x | x | x |

# 5. Discussion, conclusions and recommendations

## 5.1. Discussion - reflection

The main objective of the research was to identify the risks to the stakeholders involved in BBS.

In order to answer the main research question, it was necessary to identify the definition of BBS, who the stakeholders were, and the risks of the BBS. During the literature review, besides the definitions for BBS, stakeholders and risks have been identified. The subsequent empirical research focused on identifying stakeholders or risks empirically and unveiling the associations between stakeholders and risks.

The empirical research has identified 39 stakeholders, of which 29 were confirmed from previous literature, and 10 new stakeholders' types have been identified. The four dimensions proposed by Li et al. (2019) are applied to categorize the stakeholders represented by this research. As discussed in chapter 2, it has been inferred that the dimensions from Li et al. (2019) could be applicable in a general context, even though their research was focused on the construction domain. The empirical research used these dimensions to categorize the identified stakeholders. The only stakeholder category developed differing from Li et al. (2019) dimensions was "investors". Li et al. (2019) included the stakeholders in charge of contracting the blockchain projects (clients) in the "process" category. For these stakeholders, nothing has been identified regarding their inclusion in the process. Instead, they were associated with commissioning and financing the project. Therefore they have been classified in another category. The newly identified stakeholders were categorized into two new sub-categories within the process category: facilitators and project managers related to the technical support functions and project management roles.

Regarding risks, there were 33 risks identified during the empirical research, of which 15 were newly identified risks. Some of the risks mentioned by stakeholders, such as scalability, standardization, integration with existing systems, regulatory risks, and complexity risks, have been previously classified as barriers to adoption instead of risks (Prewett et al., 2020). As in their research, the differentiation between barriers and risks is clearly stated, the results of the literature review in chapter 2 did not include barriers in the results. For this reason, when comparing the results of chapter 4 with the literature review, these risks are not considered "new" nor "confirming literature," as those results were disregarded from the literature risks list presented in chapter 2. The status of these findings remains, therefore, uncertain. Are they risks or barriers to BBS adoption? In chapter 4, however, these debatable "risks" are included in the results since they represent risks according to the interviewees' perceptions, unveiled during the empirical research.

The primary purpose of the research was to identify the risks to the stakeholders involved in BBS. The associations made between risks and stakeholders were based on the risk perception of the interviewed stakeholders. Perception of risks can be subjective and dependent on the stakeholder's expertise. As argued by Siegrist and Cvetkovich (2000), most laypeople do not have sufficient knowledge of complex technologies to be able to make risk assessments and will rely on experts for risks evaluation. An expert in one field may not be an expert in another field. Therefore, it is worth noting that the risks association has been made according to the perception of the interviewed experts who disclosed risks associated not only with their roles but also with other stakeholders' roles. As the association of risks depends on the expert's knowledge of a particular work domain, different expertise may produce different perceptions of risks. One example is the risk perception of one interviewed stakeholder, DM03, an experienced developer. As a developer, the risks mentioned associated with his role are smart code risks (related to the risks of monetary loss due to insufficient coding), bugs risks (due to insufficient coding tests), and risks related to the project management, such as timing and technical functionalities (being the risk that the project will not finalize on time having the functionalities required). This perception is different from interviewee DM06, who associated various other risks, besides coding risks, to the group that includes developers such as business

continuity risks, systemic risks, data privacy risks, governance risks, and a few other infrastructure risks. DM06, as a project manager, has mentioned risks in a broader view of the project. However, it is not clear if the developers are directly associated with these risks or indirectly related to them, in the view only of the project manager who evaluates the risks of the entire project. Validating these peculiarities encountered in the results was not in the scope of this research. Further studies could concentrate on evaluating stakeholders' risks related only to their own roles to avoid assumptions concerning risks in other work domains.

## 5.2. Conclusions

The empirical research has identified 39 stakeholders categorized into six categories: Technical Stakeholders, Political Stakeholders, Process stakeholders, investors, social groups, and others. Four of the main categories are empirical confirmation from the dimensions described by Li et al. (2019) in the construction domain. However, this research applied it to a general context.

There were 33 risks identified during the empirical research, of which 15 were newly identified risks, as disclosed in section 4.4.2. The identified risks have been categorized into eight principal categories: Criminal use, technical, privacy, legal, human, financial, business case, and economic risks.

The main contribution of this research is the framework that discloses the risks associated with the stakeholders, which answers the main research question, as disclosed in section 4.4.3. The resulted framework allocates risks to the stakeholder, without limiting the focus on a specific domain, with the collaboration of professionals active in different industry types. However, the limitation of this study is that the experiences and risks perceptions gathered during the empirical research are related to a small number of participants.

## 5.3. Recommendations for practice

The practitioners could use the information from this research as a guideline. The stakeholders and risks have been categorized and associated. The framework can assist professionals intending to gather information about the risks related to the stakeholders involved in BBS when considering risk assessment for future adoption. Not yet all types of stakeholders are included, nor all the risks; however, they can be used as a starting point for risk analyses.

## 5.4. Recommendations for further research

This research has attempted to reveal the risks associated with the stakeholders involved in a BBS.

As this is a first attempt to produce a framework including stakeholders and their related risks, further studies could expand the research by including more participants.

Further studies could focus on the risks for the stakeholders' own roles and collect stakeholders' risks perceptions based on their own experiences. As discussed previously, narrowing the scope will prevent the interviewed stakeholder from assuming the risks to other stakeholders' roles.

Another topic for further research could be to explore the end-users stakeholder category. This category is heterogeneous, and the roles may vary depending on the domain and business processes involved. In the same way, the risks involved might also depend on the activities developed by each type of end-users. Therefore, further research could focus on end-users ' risks to better understand the risks involved for this diverse category.

# References


Alles, M., & Gray, G. L. (2020). “The first mile problem”: Deriving an endogenous demand for auditing in blockchain-based business processes. *International Journal of Accounting Information Systems, 38*, 100465.

Buth, M. C., Wieczorek, A. J., & Verbong, G. P. J. (2019). The promise of peer-to-peer trading? The potential impact of blockchain on the actor configuration in the Dutch electricity system. *Energy Research & Social Science, 53*, 194-205. doi:https://doi.org/10.1016/j.erss.2019.02.021

Butijn, B.-J., Tamburri, D., & Heuvel, W.-J. (2020). Blockchains: A Systematic Multivocal Literature Review. *ACM Computing Surveys, 53*(3), 1-37. doi:10.1145/3369052

Cagigas, D., Clifton, J., Diaz-Fuentes, D., & Fernandez-Gutierrez, M. (2021). Blockchain for Public Services: A Systematic Literature Review. *IEEE access, 9*, 13904-13921. doi:10.1109/access.2021.3052019

Calderón, J., & Stratopoulos, T. C. (2020). What Accountants Need to Know about Blockchain. *Accounting Perspectives, 19*(4), 303-323.

Daramola, O., & Thebus, D. (2020). Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting for National Elections. *Informatics (Basel), 7*(2), 16. doi:10.3390/informatics7020016

Diaz, M., Soler, E., Llopis, L., & Trillo, J. (2020). Integrating Blockchain in Safety-Critical Systems: An Application to the Nuclear Industry. *IEEE access, 8*, 190605-190619. doi:10.1109/ACCESS.2020.3032322

Drljevic, N., Aranda, D. A., & Stantchev, V. (2020). Perspectives on risks and standards that affect the requirements engineering of blockchain technology. *Computer Standards & Interfaces, 69*, 103409. doi:10.1016/j.csi.2019.103409

Fedorov, A. K., Kiktenko, E. O., & Lvovsky, A. I. (2018). Quantum computers put blockchain security at risk. *Nature, 563*(7732), 465-467. doi:10.1038/d41586-018-07449-z

Fosso Wamba, S., Kala Kamdjoug, J. R., Epie Bawack, R., & Keogh, J. G. (2020). Bitcoin, Blockchain and Fintech: a systematic review and case studies in the supply chain. *Production planning & control, 31*(2-3), 115-142. doi:10.1080/09537287.2019.1631460

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management, 51*, 102029.

Gochhayat, S. P., Shetty, S., Mukkamala, R., Foytik, P., Kamhoua, G. A., & Njilla, L. (2020). Measuring Decentrality in Blockchain Based Systems. *IEEE access, 8*, 178372-178390. doi:10.1109/ACCESS.2020.3026577

Goldfeder, S., Kalodner, H., Reisman, D., & Narayanan, A. (2018). When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. *Proceedings on Privacy Enhancing Technologies, 2018*(4), 179-199. doi:10.1515/popets-2018-0038

Islam, A. N., Mäntymäki, M., & Turunen, M. (2019). Why do blockchains split? An actor-network perspective on Bitcoin splits. *Technological Forecasting and Social Change, 148*, 119743.

Jaoude, J. A., & Saade, R. G. (2019). Blockchain Applications – Usage in Different Domains. *IEEE access, 7*, 45360-45381. doi:10.1109/ACCESS.2019.2902501

Kliem, R. L. (2000). Risk management for business process reengineering projects. *Information Systems Management, 17*(4), 71-73.

Li, J., Greenwood, D., & Kassem, M. (2019). Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. *Automation in construction, 102*, 288-307. doi:10.1016/j.autcon.2019.02.005

Lu, C., Batista, D., Hamouda, H., & Lemieux, V. (2020). Consumers' Intentions to Adopt Blockchain-Based Personal Health Records and Data Sharing: Focus Group Study. *JMIR Form Res, 4*(11), e21995. doi:10.2196/21995

Lu, H., Huang, K., Azimi, M., & Guo, L. (2019). Blockchain Technology in the Oil and Gas Industry: A Review of Applications, Opportunities, Challenges, and Risks. *IEEE access, 7*, 41426-41444. doi:10.1109/access.2019.2907695

Morganti, G., Schiavone, E., & Bondavalli, A. (2018, 8-10 Oct. 2018). *Risk Assessment of Blockchain Technology.* Paper presented at the 2018 Eighth Latin-American Symposium on Dependable Computing (LADC).

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from https://git.dhimmel.com/bitcoin-whitepaper/v/a5f36b332cb6a5fa9e701886f376ac1ac2946d07/

Nanayakkara, S., Perera, S., & Senaratne, S. (2019). *Stakeholders' perspective on blockchain and smart contracts solutions for construction supply chains.* Paper presented at the CIB World Building Congress.

Nguyen, S., Chen, P. S.-L., & Du, Y. (2020). Risk identification and modeling for blockchain-enabled container shipping. *International journal of physical distribution & logistics management, 51*(2), 126-148. doi:10.1108/ijpdlm-01-2020-0036

Osmani, M., El-Haddadeh, R., Hindi, N., Janssen, M. F. W. H. A., & Weerakkody, V. (2020). Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis. *Journal of enterprise information management, ahead-of-print*(ahead-of-print). doi:10.1108/JEIM-02-2020-0044

Pillai, B., Biswas, K., & Muthukkumarasamy, V. (2020). Cross-chain interoperability among blockchain-based systems using transactions. *Knowledge engineering review, 35*. doi:10.1017/S0269888920000314

Pincheira, M., Vecchio, M., Giaffreda, R., & Kanhere, S. S. (2021). Cost-effective IoT devices as trustworthy data sources for a blockchain-based water management system in precision agriculture. *Computers and electronics in agriculture, 180*. doi:10.1016/j.compag.2020.105889

Pouloudi, A. (1999). *Aspects of the stakeholder concept and their implications for information systems development.* Paper presented at the Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences. 1999. HICSS-32. Abstracts and CD-ROM of Full Papers.

Prewett, K. W., Prescott, G. L., & Phillips, K. (2020). Blockchain adoption is inevitable—Barriers and risks remain. *Journal of Corporate Accounting & Finance, 31*(2), 21-28. doi:10.1002/jcaf.22415

Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students. In: Pearson.

Schlegel, M., Zavolokina, L., & Schwabe, G. (2018). *Blockchain technologies from the consumers' perspective: what is there and why should who care?* Paper presented at the Proceedings of the 51st Hawaii international conference on system sciences.

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for information, 22*(2), 63-75.

Siegrist, M., & Cvetkovich, G. (2000). Perception of Hazards: The Role of Social Trust and Knowledge. *Risk Analysis: An International Journal, 20*(5), 713-720. doi:10.1111/0272-4332.205064

Tesselhof, K., Kusters, R., Janssens, G., & Veuger, J. (2020). A Proposed Conceptual Framework for Blockchain Systems. In *Blockchain Technology and Applications II*: Nova Science Publishers, Inc.

Tran, N. K., Ali Babar, M., & Boan, J. (2021). Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs. *Journal of Network and Computer Applications, 173*. doi:10.1016/j.jnca.2020.102844

Unalan, S., & Ozcan, S. (2020). Democratising systems of innovations based on Blockchain platform technologies. *Journal of enterprise information management, 33*(6), 1511-1536. doi:10.1108/jeim-07-2018-0147

Verschuren, P. J. M., & Doorewaard, H. (2007). *Het ontwerpen van een onderzoek*: Lemma.

Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration, 13*, 32-39.

Werner, F., Basalla, M., Schneider, J., Hays, D., & Vom Brocke, J. (2021). Blockchain Adoption from an Interorganizational Systems Perspective – A Mixed-Methods Approach. *Information Systems Management, 38*(2), 135-150. doi:10.1080/10580530.2020.1767830

White, B. S., King, C. G., & Holladay, J. (2020). Blockchain security risk assessment and the auditor. *Journal of Corporate Accounting & Finance, 31*(2), 47-53. doi:10.1002/jcaf.22433

Wu, J., & Tran, N. (2018). Application of Blockchain Technology in Sustainable Energy Systems: An Overview. *Sustainability, 10*(9), 3067. doi:10.3390/su10093067

Xu, Q., Xu, Q., Jin, C., Jin, C., Rasid, M. F. B. M., Rasid, M. F. B. M., . . . Aung, K. M. M. (2018). Blockchain-based decentralized content trust for docker images. *Multimedia tools and applications, 77*(14), 18223-18248. doi:10.1007/s11042-017-5224-6

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., . . . Rimba, P. (2017, 3-7 April 2017). *A Taxonomy of Blockchain-Based Systems for Architecture Design.* Paper presented at the 2017 IEEE International Conference on Software Architecture (ICSA).

Yeung, K., & Galindo, D. (2019). Why do Public Blockchains Need Formal and Effective Internal Governance Mechanisms? *European Journal of Risk Regulation, 10*(2), 359-375. doi:10.1017/err.2019.42

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2018). THE DISTRIBUTED LIABILITY OF DISTRIBUTED LEDGERS: LEGAL RISKS OF BLOCKCHAIN. *University of Illinois law review, 2018*(4), 1361. Retrieved from http://openuniversiteit.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwlV1Lj9owELZKT5Wqvh_0scqhj8MqKHYcklTqAShbsqBSQfbQU2Q7zgp1N1ttstq_3xknJAGpFXuxILZC8DeMZ4aZbwhx2cCx93RCJrlUQynBevYDwRScikyxTGeOrxhNDZUnAH_qnq4wvh9vS2NMtUm-uRSiGOQX_4243Q1ruAZoY-3sHfBubgoX4DWgDiPgDuNhyM-mx9-idbyKxmegl0A_jcbRIop_YYbPzgTSIa_WGBRYTL9jqkS0npte5uPFcjKfzEbRj67xupvEESGb99WmOL4Qt3UFTBOF1iU4zSZUCir1dydeWv2TXKV0g4r92cpbXXhTG_RV3t82HEFN7gRrndd_PEk3nwRVG_OHdhhWHJsDXanekDMbzc2ubsZP6Egh76ha6lYs7nt02SMP4zIs5MNPSJ5-mW5U-VXn9tm6R3qg0DCgM1t2SmdN-93mgZqTec8MgeO3tjniJ-RR7SxYowrjp-Sezp-R3kLcPidzQNnqgGk1KFvLk92JCuUvlsHYMhjjmhbjFyQ-mcaTmV03xrDPqetxm0smXZUGQUiFT7lygsxHswPeae6ITCkVSi4CAd6v5MxXWsH5KjwF7i2T2n1JHgqsn8hLU2eZviZWSFkqKBdZJnyeBcOAer5yXB0oHoTSZX3yEfclqVujwlBg8Kg4FzdFkbSb3ievzDr8uZTXQiWdmc87M6Ku_7jKNVKQ7dzjQ3fzkz8V70pisg9C6gWVZ9sn9JBlk5rrHjkeyjcHfo235EEr3O_I_fL6Rr8nj01Hu62E6015ZNyvIyNSfwFjg4Sx

Zhang, J., Zhong, S., Wang, T., Chao, H.-C., & Wang, J. (2020). Blockchain-based systems and applications: a survey. *Journal of Internet Technology, 21*(1), 1-14.

# Appendix 1 - Keywords used for literature research

The following keywords have been used to build the search queries for the literature review. The keywords have been identified during the initial literature review in chapter 1.

| Research Question | Key words used to build the search strings |
|---|---|
| RQ1: What are blockchain-based systems? | - blockchain-based system*<br>- blockchain system*<br>- DEFIN* |
| RQ2: Who are the stakeholders of the blockchain-based systems? | - blockchain-based system*<br>- blockchain system*<br>- blockchain network<br>- stakeholder*<br>- actor* |
| RQ3: What are the risks of the blockchain-based systems? | - blockchain-based<br>- blockchain-based system*<br>- blockchain*<br>- blockchain system*<br>- blockchain network<br>- risk* |

Variations of the keywords were considered in order to perform a broader search. The wild card represented by the symbol "*" is used to search for word variations. For instance, the keyword "DEFIN*" will find terms as "**DEFIN**itions" but also "**DEFIN**ed". Additionally, it will also provide words variations as plural.

# Appendix 2 - Literature review Blockchain-based Systems

**Tesselhof et al. (2020)** are the only identified authors who have performed a systematic literature review with the objective to create taxonomy and definitions related to blockchain-based systems. Their work is the only one that presents an explicit definition for Blockchain-based systems, which according to the results of their research it is defined as "A decentralized network where transactions can be executed." Their work is essential for this research and is considered a basis for further comparison. Their work is included as part of the conclusions in section 2.3.1.

**Fosso Wamba, Kala Kamdjoug, Epie Bawack, and Keogh (2020)** do not include definitions related to Blockchain-based systems. They have performed a systematic literature review where the term blockchain (general term) has been included. The authors do not conclude about any unique definition of blockchain that could be compared to the blockchain-based system definition from Tesselhof et al. (2020). Instead, Fosso Wamba et al. (2020) have only classified the several "blockchain" definitions encountered in the literature into three main classes: i) Holistic; ii) Ledger; iii) Database.

Frizzo-Barker et al. (2020) have classified the different literature definitions of "blockchain" into eight main groups: i) Distributed or Decentralized Ledger; ii) Trust, Security, and Transparency; iii) Chain of blocks; iv) Peer-to-peer; v) Bitcoin or Cryptocurrency; vi) Disruptive Technology; vii) value transfer; viii) infrastructure. None of these classes have explicitly related to the definition of Blockchain-Based Systems or blockchain systems.

**Gochhayat et al. (2020)** have measured the level of decentralization in Blockchain-based systems. They argue that a decentralized system does not necessarily present decentralized control when control can be exercised by a subsystem part of the application, having a centralization effect that will undermine the decentralized design. Even though their study is about blockchain-based systems, they have not defined it. In their study, the definition used is using the term blockchain associated to decentralized systems: "A Blockchain is a special kind of distributed and decentralized system, which helps users or nodes, who cannot trust each other, to reach a consensus without relying on a single centralized controlling entity" (Yang et al., 2019; Wazid et al., 2020, in Gochhayat et al., 2020). The definition used is not their own definition and is limited to only one concept of blockchain-based systems, the decentralization.

**Tran et al. (2021)** listed three main properties of blockchains: i) decentralized system; ii) trustless system; iii) immutable ledger. When discoursing about how blockchains work and presenting their architecture, Tran et al. (2021) described that blockchains use cryptographically secured systems and have a network architecture based on a peer-to-peer system. Their work is mainly concerned with blockchain technology applied to the Internet of Things. They have not identified a single definition that could be explicitly applied to blockchain-based systems.

**Wu and Tran (2018)** describe that "the Blockchain technology is not a single technology; it is a comprehensive technical system that integrates various research results." Viewing the blockchain technology as a comprehensive system, Wu and Tran (2018) describe six layers that compose the architecture of the system: Data layer, Network layer, Consensus layer, Incentive layer, Contract layer, Application layer (Yuan and Wang, 2016, in Wu & Tran, 2018). The authors also describe five characteristics of the "blockchain", which can be interpreted as characteristic of the blockchain-based system, due to the system components present in each of the characteristics' descriptions: i) Decentralization, ii) Openness, iii) Automatic execution of the contract, iv) Traceability, data temper protection, security, credibility v) anonymity. The author did not conclude about their definition, and the definitions used did not describe the same concepts as the definition of blockchain-based systems made by Tesselhof et al. (2020)

The concepts used in the definitions described by all the authors mentioned above reinforce the statement from Birch, Brown, & Parulava, who stated that "the term blockchain means too many

different things to different people" (Birch, Brown, & Parulava, 2016, in Frizzo-Barker et al., 2020). It is also in alignment with Narayanan and Clark, who have considered 'blockchain' as "an umbrella term for a class of systems that shares the same characteristics as Bitcoin" (Narayanan and Clark, 2017, in Tran et al., 2021).

**Butijn et al. (2020)** have presented a systematic literature review concerned with the "blockchain technology" concept. However, they have pointed out, in fact, to an analysis of the interconnected and interdependent systems that are part of the network where the blockchain technology is deployed, the blockchain-based systems. Further details on the analysis of their research are included as conclusions for the RQ1 in section 2.3.1.

# Appendix 3 - Literature review: Stakeholders of the blockchain-based systems

**Unalan and Ozcan (2020)** analyzed the actors that may interact with innovation systems as Blockchain systems. Their conclusion is a clustering of actors into a network of actors, which will interact with the systems, distributed by domains: Network of industry ( supply chain, entertainment, e-commerce, accounting, manufacturing, notary, etc.), Network of financial actors ( Banks, Finance Institutions, etc.), Network of Citizen ( creative consumers, user innovators, collaborative innovators), Network of Intermediaries (Professional associations, Industrial Associations, Trade Unions, etc.), Network of State (law enforcement, Government Organizations), Network of academia (University, Research Organizations, Blockchain-based science). In summary, their research highlights the potential of adherence of the entire Society to this technological innovation system, the blockchain systems. They have split the actors into a network of actors per domain of business which are interconnected.

**Cagigas et al. (2021)** have identified three types of blockchain systems' stakeholders applied to the public services domain: governments, civil servants, and citizens.

**Buth et al. (2019)** have identified various individual actors' parts of the electricity systems network included in the electricity blockchain system and actors' roles involved in the blockchain-based electricity systems adopted. As they have not identified general stakeholders and are only domain-specific, the results have not considered them.

**Li et al. (2019)** have proposed a model identifying the blockchain systems actors within the construction domain. The authors use DLT (distributed ledger technology) to describe the blockchain systems and identify their actors within the construction domain. Li et al. (2019) have identified 16 stakeholders within the construction domain, split into four domains: technical, policy, process and social. According to Li et al. (2019), the stakeholders included in the technical dimension deal with all technical aspects that a system requires to function; the policy dimension comprehends the stakeholders within the environment in which the BBS are inserted, such as regulations, laws, policies, standards, and compliance. The stakeholders included in the process dimension are related to all business practicalities related to the organization considering the implementation of BBS. The social dimension focuses on the social impact of BBS integrated with real-world concerns such as the effects of data protection regulation or environmental sustainability. It can be argued that the description of the dimensions proposed by Li et al. (2019) can be broadly applied and are not limited to the construction domain.

**Diaz, Soler, Llopis, and Trillo (2020)** describe the process of safety inspection based on a blockchain system. The stakeholders mentioned are the company owner of the plant, inspection companies and the regulatory body, besides the stakeholders related to the internal business network that is part of the process execution object of the inspection. The business network roles and responsibilities are defined by the granted permissions and access to the blockchain, which allows the execution of the internal business processes into the blockchain. This research is a case study and has analyzed a permissioned blockchain system. As they have not identified general stakeholders and only domain-specific, it has not been included in the results

**Islam, Mäntymäki, and Turunen (2019)** have researched the bitcoin network using the lens of the actor-network theory. They have identified eight actors in the blockchain network: the blockchain itself, miners, core developers, exchange/marketplace owners, investors, merchants, hardware manufacturers, and wallets. These actors are classified into three dimensions: social, technological, and economical. The dimensions represent the heterogeneity of individual actors and the different

functions that each actor represents in the network. Their research is, however, only focused on the bitcoin network.

**Pincheira, Vecchio, Giaffreda, and Kanhere (2021)** refer to Internet of Things (IoT) devices as direct actors in a public blockchain network, using a smart contract structure in the management of water supply systems. The authors argue that the permissionless blockchain supports the interests of water management stakeholders. However, besides the direct stakeholders represented in the system by IoT devices, their research has not listed any other stakeholders.

# Appendix 4 - Literature review: Risks of the blockchain-based systems

**Prewett et al. (2020)** have discussed barriers and risks to the adoption of blockchain-based systems. They argued that barriers are factors and deficiencies that prevent companies and industries from adopting the blockchain technology. On the other hand, risks are related to vulnerabilities or circumstances not foreseen when dealing with the adoption of the blockchain system. Due to the clear differentiation between barriers and risks, every time these barriers were considered risks in other research papers, they have not been considered in the literature review results. Prewett et al. (2020) mentioned five barriers to the adoption of blockchain systems: Scalability; blockchain systems lack of integration with legacy systems; lack of coding standardization and, in consequence, lack of interoperability between systems; complexity of blockchain applications; regulatory uncertainty; lack of knowledge, skills, and training;

The risks listed in their research were:

**Architecture and design risks** are related to the design or coding choice made related to systems and, for example, i) consensus mechanisms on the public blockchain or ii) access restriction and roles differentiation on the consortium type blockchains. All the design choices must be exhaustively tested before being put into production.

**Endpoint risks** are the interfaces where humans and machines interact in the network. It is where data is captured, created, and transmitted. The interface is made by every connected device, a string of code, or human interaction, which introduces risks.

**Data Security and confidentiality risks**: is related to the physical and logical access made by private keys. Additionally, the development of quantum computing also represents risks to the current encryption algorithms and consequently present risk to the confidentiality of the data.

**Storage:** Independent of the storage approach taken, the company should consider a long-term storage plan and the associated costs.

**Smart contract risks:** the smart contract will act according to the logic programmed therein and not in accordance with the developers' intention. If it is not properly developed, coded, and tested, it will launch undesired outcomes and broadcast to the entire network.

**Compliance risks**: lack of global standards where each jurisdiction may adopt different standards. Each participant node might be subject to different standards in different jurisdictions.

**Vendor risks**: services providers may have weaknesses in the security, code used, or lack appropriate personnel, which can expose the contracting organization to risks.

**Contractual risks:** are related to the development and administration of contracts related to blockchain deployment. Rights per participant in the network can vary and are defined on the services agreements.

**Private key management:** digital assets could become irretrievable if a private key is lost. It is also possible that a private key is stolen, and in this case, the thief has access to the assets.

**Goldfeder, Kalodner, Reisman, and Narayanan (2018)** discussed the privacy risks related to web purchases made from crypto wallets. They have concluded that it is possible to identify the wallets' address in the blockchain after web purchases and establish the link to personal identity details. The identification is made based on the trackers (cookies) placed on the personal computers by the merchant websites.

**Nguyen, Chen, and Du (2020)** discuss the operational risks for the cargo shipment domain. The risks included in their research are in its majority related to the business process management cycle, the phase before the information is included in the blockchain system. These are risks of the business processes, such as reconciliation and reporting, are not blockchain systems risks. Therefore, these risks have been disregarded. The relevant blockchain system risks considered by the authors are: Instability of the cloud platform blockchain provider; Cyber-attacks on the blockchain or the local IT

systems before the execution of the smart contracts; Smart contract errors; misuse of weakness in the smart contract set up; stolen identity; risks of errors in the interface with the real world such as human interaction, sensors, and other devices;

**Fedorov, Kiktenko, and Lvovsky (2018)** discussed the risks when, in the future, quantum computers would decipher the cryptography algorithms currently used.

**White et al. (2020)** describe the inherent risks that should make part of an auditor assessment of the blockchain systems. The risks are categorized into: technological, data security, interoperability, and third-party vendor risks. These authors categorize interoperability as a risk. However, as discussed before, this is considered a barrier to adoption, according to Prewett et al. (2020).

**Zetzsche et al. (2018)** discussed the legal aspects and liabilities related to BBS. The risks identified were categorized into ledger transparency, cyber, and operational risks of the BBS. Ledger transparency risks are data privacy, insider trading, market abuse and identity theft. Cyber risks are tampering data, brute force attacks and cheats, double-spending attacks and denial of service attacks. Operational risks are insufficient coding, key person risk, negligent performance.

**Drljevic, Aranda, and Stantchev (2020)** have reviewed grey literature based on business reports from consultancy firms. Their review lacks a discussion about the context of each named risk. Therefore it has not been included in the literature review results.

**H. Lu, Huang, Azimi, and Guo (2019)** split risks into three categories: operational risks, cyber risks, and legal risks. Operational risks are Loss of data and identity; The transaction costs of the public blockchain are high; Lack of recipients and users; Lack of long-term experience, leads to underperformed management; Initial applications may have technical problems, Lack of a standardized mode of operation, function, and security deficiencies.

Cyber risks due to bad behavior or insufficient security are fraud risks on the interface between the real world and the blockchain world; The exchange may be attacked by hackers, and the user's

password may be hacked and funds transferred, the hard fork of the block will cause the trust of the entire network system to be questioned.

Legal risks listed are related to illegal acts that may occur in the operation of blockchains; it is reflected in: Tax evasion may be triggered, Illegal use of information, Blockchains are used for illegal transactions. This research, however, is related to the oil and gas domain. The listed risks are based on financial markets/bitcoin blockchain risks literature. Due to the lack of consistency perceived, this research has not been included in the conclusion.

**Osmani, El-Haddadeh, Hindi, Janssen, and Weerakkody (2020)** have mentioned five types of challenges: scalability, security risks, reversibility, interoperability, regulatory risks. As a result of the research, these challenges are classified into risks, proving the interchangeable use of these two concepts (challenges and risks), causing some discrepancy. Besides, some of these categories (scalability, interoperability, and regulatory uncertainty) were considered by **Prewett et al. (2020)** as barriers to adoption instead of risks. Due to the presented discrepancy, the results of this research have not been included in our conclusion.

**Cagigas et al. (2021)** have identified three types of blockchain systems' stakeholders applied only to the public services domain: governments, civil servants, and citizens. This article has been used from the results of the literature review of the RQ2 since for the identified stakeholders they have also identified a list of risks and challenges with a stakeholders-centric approach, which are a) Risks for Governments: interoperability risks, jurisdiction legal risks, privacy compliance risks, scalability constraints, uncertain about acceptance of the blockchain systems as a trust mechanism. From this

list, only jurisdiction legal risks and privacy risks are considered in the result. The other ones have characteristics of barriers instead of risks. b) Risks for civil servants: the items mentioned by the authors under the civil servants' risks are debatable since they are not risks of the systems, but are costs to the adoption such as lack of skills and knowledge to use the systems and necessary culture change. Besides this, also the reduction of jobs is mentioned as a risk. However, it concerns the application and use of new technology in general, not directly related to BBS. Therefore, none of the items considered as risks for the civil servants have been considered in the results. c) Risks for citizens: Security risks; Lack of flexibility; Trustworthy reputation, reidentification risks (privacy), minority groups of experts in the lead of governance, lack of knowledge and skills, lack of resources. From this list, only security risks, privacy risks, data quality and governance risks are considered in the results, as the other ones mentioned are considered barriers to adoption, as previously discussed.

# Appendix 5 - Source types details

Different sources of information can be used to perform empirical research. Verschuren and Doorewaard (2007) mention five types of sources: a) people; b) media; c) observation and/or measurement of real situations; d) documents; and e) literature. These authors highlight that people might be the most important source of information in research since they can provide information that can be collected in a shorter time than other sources. Considering that this research is interested in people (stakeholders) and their perceptions of risks, "people" is considered the primary source of information. Media information is considered "gray" literature and is not allowed in this master research. Real situation observation is not applicable to answer the empirical research questions, which are concerned with identifying stakeholders, risks, and stakeholders' risks. Therefore observation of real situations is not applicable. Documents could also be used as a source of information. In the case of this research, documents can be seen as a secondary source of information to perform triangulation with the information provided by people, but it will not be considered the main source of information. It considers that once people accept participating, they can provide information according to their experience. However, documents will vary from stakeholder to stakeholder and are probably not in a format that can be compared between participants. Therefore, people are chosen as the main source of information for this research.

# Appendix 6 - Interview questions design and motivations

| Theme | Interview Questions | Motivation of the question |
|---|---|---|
| Introduction | 1. What type of blockchain-based systems are you involved with? | This question provides background details of the stakeholder and the type BBS they are involved with. |
| | 2. What is your role in relation to this blockchain-based system? | This question provides background details of the stakeholder and their role in a BBS. |
| Stakeholders of Blockchain based systems | 3. Could you please list the stakeholders of the blockchain-based systems in which you are involved with? | This question provides direct answer to the empirical question number I . |
| | 4. Who are the stakeholders you frequently work with? | This question requires a reflection on the question above and request details of the stakeholders related to the interviewed stakeholder. |
| | 5. What are the roles of the involved stakeholders ? | The role of the stakeholder will provide details for comparison with practice and definitions of the stakeholders in the literature. As expected the names can vary, and the roles description will provide additional information. |
| | 6. Do you have any documentation confirming the given answers ? | If available docs can be used to perform triangulation. |
| Risks of the blockchain based systems | 7. Could you please list the risks of the blockchain based systems in which you are involved with ? | This question provides answer to the empirical question number II |
| | 8. Why do you think this is a risk ? | This question requires further consideration on the answers provided above. |
| | 9. What are the risks related to your own role? | This question provides the opportunity for the direct answer to the empirical question III, related to the stakeholder being interviewed. |
| | 10. Do you have any documentation confirming the given answers ? | If available docs can be used to perform triangulation. |
| Risks for the stakeholders of the blockchain based systems | 11. Which of the identified risks are associated by the identified stakeholders? | This question provides the opportunity for the direct answer to the empirical question III, according to the experience of the interviewed stakeholder. |
| | 12. Do you have any documentation confirming the given answers ? | If available docs can be used to perform triangulation. |

# Appendix 7 - Profile of participants

Some criteria are established to select participants that will be invited for the semi-structured interviews. The participants (stakeholders of BBS) should be professionals that have been involved with BBS, varying from development, design, implementation, use, governance, mining, research, policy, social groups, etc. This is the practical interpretation adopted when following the definition from Pouloudi (1999, p. 8) used in this research: "A stakeholder of an interorganizational system is any individual, group, organization or institution who can affect or be affected by the interorganizational system under study" (Pouloudi, 1999, p. 8). The stakeholders should have (or have had) involvement with BBS in a recent period, as recent as a maximum of two years. This requirement aims to avoid collecting outdated information since the technology is evolving quickly. The participants should have at least three years of professional experience, as risk assessment requires expertise in a work domain.

# Appendix 8 - Email approaching potential participants

Dear “X,”
Thanks for allowing “Y” to share your contact details with me.

My name is Daniela, and at this moment, I am working on my master thesis from the Master in Business Process Management & IT at the Open Universiteit. The research theme is “what are the risks to the stakeholders in a blockchain-based system?”.

For this research, I am searching for people that are willing to participate in a 1-hour interview that will take place in September.
The profile of the interviewees are stakeholders that have been involved with the adoption of blockchains systems (developers, business leaders, project leaders, project team members, users, system architects, etc.). Any stakeholders that have been involved with the adoption or preparing for the adoption of blockchain systems. Anyone that can speak with us about the perception of risks considered by the implementation or risks identified during the use of blockchain systems. If the systems are not implemented yet, it would be interesting to identify the risks being considered related to future adoption.

Important to mention that the information gathered at the interview will be used for academic purposes only.

The interviews round will take place somewhere in September (the exact dates will be agreed upon later). At this moment, I am searching for participants. It would be wonderful if you could contribute with your insights.

Would you accept to participate?

I am looking forward to hearing from you!

Thanks in advance,

Kind regards,

Daniela

# Appendix 9 - Participant's interview protocol and questions

## Interview protocol

Dear Participant,

You are receiving this interview protocol in advance of the agreed interview related to the field research for the master thesis "What are the risks to the stakeholders involved with blockchain-based systems? ". The master thesis is part of the master's study in Business Process Management & IT at the Open Universiteit in Amsterdam. This interview protocol contains details of the research concepts and guidelines for the interview. The goal of the research is to investigate what are the risks associated with each type of stakeholder.

The interview will take approximately one hour. Upon your consent, the interview will be recorded to my computer using Zoom. It is important to mention that any information provided to us will be used for academic purposes only. After the interview, the interview will be transcribed. Interview transcripts will be anonymized in order to keep your privacy in relation to the interview data. Upon completion of the research, the interview records will be deleted. The anonymized transcripts will be kept for research purposes.

The interview is based on three main concepts: blockchain-based systems, stakeholders, and risks.

Please find below the definitions used:

**Blockchain-based systems**: Blockchain-based systems are a decentralized network where transactions can be executed and where the Blockchain technology, a form of distributed ledger technology, is deployed (Butijn et al., 2020, Tesselhof et al., 2020).

**Stakeholder: "**A stakeholder of an interorganizational system is any individual, group, organization or institution who can affect or be affected by the interorganizational system under study"(Pouloudi, 1999, p. 8).

**Risks**: "Risk is the probability of occurrence of an event that has some consequences" (Kliem, 2000).

It is important to mention that you, as a participant, may interrupt the interview at any time.

Please inform me if there are any questions. If not, we will proceed with the interview.

Could you please confirm that you agree with the recording of the interview? If yes, the recording of the interview may start.

The interview questions are as follows:

| Theme | Interview Questions |
|---|---|
| Introduction | 1. What type of blockchain-based systems are you involved with? |
| | 2. What is your role in relation to this blockchain-based system? |
| Stakeholders of Blockchain based systems | 3. Could you please list the stakeholders of the blockchain-based systems in which you are involved with? |
| | 4. Who are the stakeholders you frequently work with? |
| | 5. What are the roles of the involved stakeholders ? |
| | 6. Do you have any documentation confirming the given answers ? |
| Risks of the blockchain based systems | 7. Could you please list the risks of the blockchain based systems in which you are involved with ? |
| | 8. Why do you think this is a risk ? |
| | 9. What are the risks related to your own role? |
| | 10. Do you have any documentation confirming the given answers ? |
| Risks for the stakeholders of the blockchain based systems | 11. Which of the identified risks are associated by the identified stakeholders? |
| | 12. Do you have any documentation confirming the given answers ? |

# Appendix 10 - Interview procedures - protocol

1.1 The interview is scheduled for one hour.
1.2 At the beginning of the interview, the researcher will introduce himself and the subject of the research in progress.
1.3 The researcher will ask if the interviewee has read the participant's protocol (Appendix 9).
  1.3.1 In case the participant has not read the protocol, the researcher will read it and discuss it entirely before the interview, with the goal that the participant will understand the concepts of the research, topics of the interview questions, privacy provisions and further guidelines included in the protocol, besides certifying that there are no further questions.
  1.3.2 If the participant answers that he/she has already read the protocol, the researcher will briefly discuss each paragraph of the protocol, in any case, to make sure that the participant has understood it and that there are no further questions.
1.4 In the last line of the protocol, there is a request to record the interview.
  1.4.1 If the participant agrees, the recording may start.
  1.4.2 If the participant refuses to record the interview, the interview should be canceled.
1.5 After the recording has started, the interview may proceed according to the interview questions.
1.6 The researcher will share the screen in order to visualize the interview questions.
1.7 If a question is not satisfactorily answered, the researcher may state additional questions in order to seek clarification.
1.8 During the interview, the researcher will make notes in an excel sheet related to the stakeholders and risks identified. The stakeholders will be included in the Y-axis and the risks in the X-axis.
1.9 At interview question number 11, the excel sheet will be shared with the participant. The participant will be requested to associate the risks to the stakeholders in the excel sheet. By each identified risk, an "X" will be placed in the line of the identified stakeholder. The excel sheet will be discussed and filled in by the researcher.
1.10 The participant will then have the opportunity to visualize the information provided and indicate the risks related to each mentioned stakeholder.
1.11 If the participant remembers any additional stakeholders or risks, it could be included.
1.12 Once the excel sheet is completed, the researcher will continue with the last interview question, number 12.
1.13 Once all the questions are answered, the interview recording will be stopped.

The researcher will thank the participant for the time and cooperation with the research.

# Appendix 11 - Test interview results

The participants' interview protocol (Appendix 9), including the guidelines to the interview and the final interview questions, was sent a few days in advance to the interviewee.

When the zoom call started, the interviewee was asked if he had read the protocol. The answer was affirmative. Therefore, the protocol was briefly discussed per paragraph in the same sequence as in the participants' interview protocol to make sure that all topics were clear before the interview started.

Discussed topics as presented in the participant's protocol (This introduction took about 10 min):

a) The theme and the goal of the research
b) Duration of the interview and recording of the interview after consent is granted
c) Informed the participant that the interview will be transcribed later and informed the privacy procedures related to the research. To make the interviewee confident about the privacy rules, it was stressed that the research is interested in individual stakeholders' view of risks and that none of this information will be linked to any personal information or company names.
d) Concepts of the research: blockchain-based system, stakeholders, and risks.
e) The interviewee was informed that he could interrupt the interview at any time.
f) When asked if there were any questions, he had one comment. As he has read the interview questions in advance, he was concerned about the documents requested in some of the interview questions. He mentioned that he could not share any documents since they are confidential client information. It was explained that the questions would have to be made as part of the interview questions, and he was free to give any answer during the interview, also negative if necessary.
g) The researcher requested permission to record and start the interview questions.

After another team member took the first test interview, this test interview was prepared. The different concerns the rephrasing of the interview questions 3 and 7, where the words "Could you please list ..." were included to avoid too many details being provided by the participant. The rephrasing of the questions had the objective to induce a direct answer: a list of the stakeholder (question 3) or a list of the risks (question 7). This objective was achieved and the answers received were more concise for these questions.

| **Question from 1st test interview** | **Definitive question used for the final interview questions** |
|---|---|
| #3 Who are stakeholders at the blockchain-based system you use? | #3 Could you please list the stakeholders of the blockchain-based system in which you are involved with? |
| #7 What are the risks of the blockchain-based system you are using? | #7 Could you please list the risks of the blockchain-based system in which you are involved with? |

In his situation as a professional with five years BBS experience and working as blockchain services team lead for a well-known global services company, he has experience with many use cases and, for the interview, decided to mention two examples. The first one is from a BBS used for an insurance company and its respective network. The second example was a blockchain-based system used by the cosmetic industry supply chain that traces the origin of its products for ESG (environmental, social and governance) purposes. Both were private blockchains. In summary, the interview went well, all the other questions were answered accordingly, and the excel sheet was completed successfully. The interview finished within the time scheduled—no further specific remark.

# Appendix 12 - Data Analysis Protocol

**Procedure for the template creation to analyze and display the data to answer RQ1 and RQ2**:

**1. Data visualization tool to be used for the data analysis**

Miro will be the online tool to be used as it has met the following criteria's:

1.1 It is free.
1.2 It is known by at least one of the researchers, which will avoid that time spent familiarizing with a tool.
1.3 It is user-friendly and provides options for virtual post-its, replacing the paper post-its in common use.
1.4 It provides a better overview than another visualization tool tested (Trello board).

**2. Template Analysis process - planning of group meetings**

2.1 One kick-off physical meeting with the researcher's team is planned, and subsequent online meetings are scheduled to prepare the initial (a priori) template. In total, three meetings are expected to be necessary; One physical meeting of 3 hours, plus two online meetings of 1.5 hours each to complete the initial template (a priori). It is expected that the data analysis for the further development of the template based on the interviews data (in-vivo) and further categorization can be done using the same time frame.

**3. Template Analysis process- Preparation**

3.1 Each researcher should have a complete numbered/ordered list containing all stakeholders and risks resulting from the literature review, including definitions, which will be used as a reference during the meetings to create the templates.
3.2 The same process will be applied to the stakeholders and risks, using the Miro board as a tool.
3.3 Two empty boards will be created in Miro, one for stakeholders and one for risks. The boards will have the first column named "items to be categorized" and subsequent columns as Category A, Category B, etc., as needed.
3.4 Before the first meeting, all the researchers should include virtual post-its in the Miro board with all items (stakeholders and risks) that were obtained from the literature results ("a priori" codes) for both stakeholders and risks. The virtual post-its will be included in the first column of the respective boards, in the column named "items to be categorized." Each researcher should use one post-it color available in Miro to differentiate the information included per researcher.
3.5 If items are duplicated and have the same definition, the researcher should compact them into one item and reference the number from the original list for identification.
3.6 Before starting the categorization process, the other columns (category A, Category B) should be named. The initial categories names should represent main concepts founded in literature (to be refined later, as needed). These initial category names should be originated from the literature or be created by the researchers, provided that a category name has a common understanding among the researchers and that it is in line with the main subjects discussed in the literature review.
3.7 Once the initial main categories are agreed between the researchers, the columns should be named per category, and their definitions should be drafted in order to guide the categorization process. Once this is done, the categorization of the items can start.

**4. Template Analysis process - Initial template creation (a priori codes)**

4.1 The categorization process should start following item per item included on the board (stakeholders and risks), one at the time, per researcher.

4.2 The researcher will read the name of the item and its definition. Based on the item definitions, the researchers will proceed as:

4.2.1 A category can be chosen from the few initial categories created, provided all researchers agree. OR

4.2.2 If the item does not fit the existing categories or no agreement is achieved concerning the existing categories, the item is placed into the group "further discussion" and discussed at the end of the process.

4.3 At the end of the initial categorization process, the items remaining in the "further discussion" group will be analyzed to evaluate the need for new categories.

4.4 A new category may be created based on the similarities of the uncategorized/disputed items placed as "further discussion." The researchers may create codes to name a new category if no better categorization name can be found from the literature review items.

4.5 Once all the items are categorized, there should be a review per item within a category to verify if all the items were correctly classified. If inconsistencies are noticed, some reclassification may occur.

4.6 Upon confirmation of the correct categorization, the researchers should analyze the similarities of the items within a category to identify clusters, if applicable.

4.7 Based on the characteristics of the clusters, sub-categories names could be suggested, discussed and upon agreement, created. If no clusters are identified within a category, there will not be necessary to create sub-categories.

4.8 Upon creation of sub-categories, their definitions should be drafted.

4.9 An iterative review should occur every time new categories or sub-categories are created to identify if the items are still corrected categorized considering the changes made. Every time a review is performed, reclassification may be necessary.

4.10 Once the process is finished, definitions should be reviewed and refined.

4.11 A final review should confirm if the definition created applies to all items included in the category.

4.12 Upon completing all the steps mentioned above, the initial template ("a priori" phase) will be ready to be used as the basis for further categorization of the items derived from the interviews ("in vivo" categorization phase).

**5. Template analysis process - template development with interviews data (in vivo codes)**

5.1 The interview transcripts will be coded using the "in vivo coding standard form" created by the group of researchers. The form has the goal to standardize, among the researchers, the codes derived from the interview transcript.

5.2 Each researcher will fill in, per interview transcript, one standard form in vivo coding.

5.3 Each researcher will send their forms per email to all the researchers since this will be the information that will be based on the data analysis related to the interviews. All the researchers should familiarize themselves with all the data coded before the categorization process begins.

5.4 New Miro boards will be created named "results of the interviews" for stakeholders and risks, using the categories and sub-categories created in the initial template (a priori).

5.5 Each researcher will include the items related to stakeholders and risks resulting from its own "in vivo coding standard forms in the two new Miro boards." The column "uncategorized items" should be used at the start of the process.

5.6 Each item included in Miro should be referenced to the interview number for identification.

5.7 In case of duplicated items (having the same name and definition), they should be condensed into one item, including the reference number of the in vivo coding standard form.

5.8 Names that are not explicitly duplicated, but seem similar concerning context, should be analyzed by the group and reduced, if possible. In case of categories are changed or merged, there should be a track tracing the original names into the new transformed names.

5.9 At the start of the categorization process, the researchers should inform the other researchers, besides the names included in the Miro board, also their definition and context according to the “in vivo” standard form.

5.10 The categorization process for the in vivo codes will follow the same process as described for creating the initial template (“a priori” phase) related to steps 4.1 up to 4.11.

5.11 At the end of the categorization process for the in vivo codes, if there are conflicts with the original literature names, data should be replaced provided they have the same context, and the literature names should be kept.

**Procedure for data analysis and display related to RQ3:**

5.12 Once the categorization process of stakeholders and risks is finalized, all the associations of stakeholders and their respective risks identified by the interviewees will be placed into a single matrix to answer the main research question. The stakeholders (and their categories) and risks (and their categories) will be placed into the Y-axis and X-axis, respectively. The identified risks per stakeholder will be marked in the table with an “x.”

# Appendix 13 - “in vivo” coding - standard form

| | |
|---|---|
| Introduction | Interviewee <CODE> is from <COUNTRY>, is involved with <BBS PROJECT>, has the role of <ROLE IDENTIFIED>, has <NUMBER> years of experience in BBS and works in the <TYPE OF INDUSTRIE> |
| Stakeholders of blockchain-based systems | Interviewee <CODE> has identified the following stakeholders:<br>1. <STAKEHOLDER A> – <DESCRIPTION/ROLE STAKEHOLDER><br>2. <STAKEHOLDER B> – < DESCRIPTION/ROLE STAKEHOLDER ><br>Etc.<br><br>Interviewee <CODE> works frequently with the following stakeholders < INFORM THE ONES MENTIONED >.<br><br>Interviewee <CODE> <has/has not> provided documents to confirm the mentioned stakeholders. |
| Risks of the blockchain-based systems. | Interviewee <CODE> has identified the following risks:<br>1. <RISK A> – <EXPLAIN RISK><br>2. <RISK B> – <EXPLAIN RISK><br>etc.<br><br>Interviewee <CODE> has the following risks related to his role:<br><INFORM THE ONES MENTIONED>.<br><br>Interviewee <CODE> <has/has not> provided documents to confirm the mentioned risks. |
| Risks to the stakeholders of the blockchain-based system. | During the interview <CODE> the excel-sheet below has been completed to associate the mentioned risks to the mentioned stakeholders, according to the view of the interviewee.<br><br>Interviewee <CODE> <has/has not> provided documents to confirm the mentioned stakeholders’ risks. |

# Appendix 13.1 - Interview DM01 - In vivo coding

| | |
|---|---|
| Introduction | Interviewee **DM01** is from ENGLAND, is involved mainly with BITCOIN BLOCKCHAIN and ETHEREUM based public blockchains (not specified), has the role of BLOCKCHAIN ANALYTICS SERVICE PROVIDER (founder of the company), has six years of experience with BBS and works in the Technology services sector. |
| Stakeholders of blockchain-based systems | Interviewee **DM01** has identified the following stakeholders:<br>1. **TRADING OPERATORS** (private, small scale) – indirectly users of the blockchain information for trading purposes. Receive the information from the Blockchain Analytics services provider.<br>2. **ASSET MANAGERS** (of investment funds) - indirectly users of the blockchain information for trading purposes. Receive the information from the Blockchain Analytics services provider.<br>3. **BLOCKCHAIN SERVICE ANALYTICS PROVIDER** - Uses the information from the BBS to provide blockchain analytics services to clients.<br>4. **RESEARCHERS** - Working at the service analytics providers to provide information to the clients<br>5. **TRADERS** (retail) - Use information through the exchanges<br><br>Interviewee **DM01** works frequently with the following stakeholders: **2, 4**<br>Interviewee **DM01 has not** provided documents to confirm the mentioned stakeholders. |
| Risks of the blockchain-based systems. | Interviewee **DM01** has identified the following risks:<br>1. **slow & cumbersome (scalability)** – the system is very slow, being this a big risk for adoption.<br>2. **Uncertainty transactions confirmations** - there is a risk that the transaction will not complete or will take long to confirm its completion.<br>3. **Costs** - transaction fees can become expensive<br>4. **Transparency /privacy risks** - private information can be revealed.<br>5. **Regulatory risk**- uncertainties about regulations<br>6. **Reputational risks**- risks of damage to the brand<br>7. **Few barriers to entry for competitors** - because it is based on public information from the blockchain, and anyone can start doing the same.<br><br>Interviewee **DM01** has the following risks related to his role: **7**<br>Interviewee **DM01 has not** provided documents to confirm the mentioned risks. |
| Risks to the stakeholders of the blockchain-based system. | During the interview **DM01**, the excel-sheet below has been completed to associate the mentioned risks to the mentioned stakeholders, according to the view of the interviewee.<br>Interviewee **DM01** has **not** provided documents to confirm the mentioned stakeholders' risks. |

| A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|
| Stakeholders / Risks | slow and cumbersome - scalability | uncertainty - transactions confirmations | costs | too much transparency is a privacy risk | regulatory | reputational | few barriers to entry - related to competitors |
| trading operators - private smaller scale | x | x | x | x | | | |
| asset managers - investment funds | | | | x | x | x | |
| service analitycs provider | | | | | | | x |
| researchers | | | x | | | | x |
| traders - retail | x | x | x | | | | |
| | | | | | | | |
| | | | | | | | |

interview 1409 [redacted]

# Appendix 13.2 - Interview DM02 - In vivo coding

| | |
|---|---|
| Introduction | Interviewee **DM02** is from The Netherlands, is involved with the Energy Web Foundation public BBS PROJECT (peer-to-peer exchange of energy in local communities), has the function of Program Telecom Manager and the role in the project development team on the BBS project workgroup, has three years of experience in BBS and works in the energy infrastructure sector. |
| Stakeholders of blockchain-based systems | Interviewee **DM02** has identified the following stakeholders:<br>1. **Energy producer companies** – Producers of energy - interested in the balance of the energy grid<br>2. **National Grid energy distributors** – Deliver energy - interested in the balance of the energy grid<br>3. **Consumers -** Participants of the smart contracts in order to consume energy in local communities<br>4. **Prosumers** - Households (small producers) who produce energy and participate in the smart contracts delivering the energy from solar panels to the local communities.<br>5. **Regulators** - evaluate if the blockchain being used meets the rules established by the privacy laws.<br>6. **DSO - Grid management** - Interested in maintaining a balanced energy grid. The DSO controls information to ensure the demand is attended to and the grid is balanced.<br>7. **Project Development Team** - interact with the various stakeholders on behalf of the interests of the DSO.<br><br>Interviewee **DM02** works frequently with the following stakeholders: all of them.<br>Interviewee **DM02 has not** provided documents to confirm the mentioned stakeholders. |
| Risks of the blockchain-based systems. | Interviewee **DM02** has identified the following risks:<br>1. **Privacy legislation risk–** The information disclosed on the blockchain should meet the restrictions of the privacy regulations, which can be differently interpreted by National regulators and European Regulators.<br><br>Interviewee **DM02** has the following risks related to his role: The interviewee does not recognize the risk specific to him. He has focused on the privacy legislation risks that affect the other stakeholders of the project.<br>Interviewee **DM02** has not provided documents to confirm the mentioned risks. |
| Risks to the stakeholders of the blockchain-based system. | During the interview **DM02,** the excel-sheet below has been completed to associate the mentioned risks to the mentioned stakeholders, according to the view of the interviewee.<br>Interviewee **DM02 has not** provided documents to confirm the mentioned stakeholders' risks. |

| A | B |
|---|---|
| **Stakeholders / Risks** | **Privacy legislation** |
| **energy producers - companies** | x |
| **distribution - national grid - tennet** | x |
| **consumers** | x |
| **pro-sumers ( small producers)** | x |
| **regulators ( National and European)** | x |
| **Distribution Systems Operators (DSO) - grid management** | x |
| **Project Development Team** | na |
| | |

# Appendix 13.3 - Interview DM03 - In vivo coding

| | |
|---|---|
| Introduction | Interviewee **DM03** is from Finland, is involved with Ethereum BBS projects, but has also been involved with Bitcoin blockchain in the past, works as an independent consultant and has the role of solidity developer (code for smart contracts), has five years of experience in BBS and works in the consultancy sector. |
| Stakeholders of blockchain-based systems | Interviewee **DM03** has identified the following stakeholders:<br>1. **Deployer of the contract** - Commissions (or contracts) and provide funding for the creation of the smart contract<br>2. **Administrator** - IT support role that manages the contract once it is deployed (puts the contract on hold, for example, if there is a bug, or funds are stolen, or investigates any other error.).<br>3. **Exchanges** - see the contract as a commodity. They are a marketplace provider; they do not interact with the contract<br>4. **Developers** - write the code on the contract<br>5. **End-user smart contract** - customers using the smart contract<br>6. **Business management of the project** - project management (CTO)<br><br>Interviewee **DM03** works frequently with the following stakeholders: **1,4**<br><br>Interviewee **DM03 has not** provided documents to confirm the mentioned stakeholders. DM03 mentioned is committed to the confidentiality clausula on his contracts with clients and is not allowed to share documentation. |
| Risks of the blockchain-based systems. | Interviewee **DM03** has identified the following risks:<br>1. **Security code risks** - Risk that the value locked in the contract can be stolen by unauthorized people.<br>2. **Project management risk**– The risk that the project will not be finalized on time or includes all the functionalities required<br>3. **Market product fit risks** - Will the final designed product by the smart contract has acceptance in the market.<br>4. **Bugs risks** - The risk that a mistake is inserted in the code and that is not identified on time during the tests.<br><br>Interviewee **DM03** has the following risks related to his role: 4<br><br>Interviewee **DM03 has not** provided documents to confirm the mentioned risks. The same as mentioned above, DM03 is under a confidentiality clause on his contracts with clients and is not allowed to share documentation. |
| Risks to the stakeholders of the blockchain-based system. | During the interview **DM03,** the excel-sheet below has been completed to associate the mentioned risks to the mentioned stakeholders, according to the view of the interviewee.<br><br>Interviewee **DM03 has not** provided documents to confirm the mentioned stakeholders' risks. DM03 is under a confidentiality clause on his contracts with clients and is not allowed to share documentation. |

| A | B | C | D | E |
|---|---|---|---|---|
| **Stakeholders / Risks** | **security code - funds allocated to contract** | **project management risks** | **market product fit risk** | **software bugs risks** |
| **deployer - contractor ( funding)** | | x | x | |
| **administrator - IT support role** | x | | | x |
| **exchange - market place provider** | | | | x |
| **developers - write code** | x | x | | x |
| **users of the contract - costumers** | x | | x | |
| **business Management of the project - CTO** | | x | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

interview 2409 [redacted]

# Appendix 13.4 - Interview DM04 - In vivo coding

| | |
|---|---|
| Introduction | Interviewee **DM04** is from The Netherlands, is involved with the Energy Web Foundation (EWF), a public blockchain, in the proof-of-concept phase related to asset registration in the blockchain, works as a business analyst and has the role of internal advisor at the innovation department in of one of the grid management companies participating as a node in the system, has five years of experience in BBS and works in the energy infrastructure sector. |
| Stakeholders of blockchain-based systems | Interviewee **DM04** has identified the following stakeholders:<br>1. **Innovation department** – responsible for the idea, start of the project and the first design of the logic for the blockchain project.<br>2. **Telecom department** - Are the first customers of the system. They set up use cases of the assets (routers) that should be onboarded.<br>3. **Asset management** - these will be the main users of the systems since they are responsible for the management of the assets onboarded in the system (Planning life cycle of the assets and new purchases).<br>4. **Internal installers (Infrastructure)** - Deals with the installation process of the physical devices that produce information (scanned QR codes) to the blockchain. Make sure that the asset is properly identified and authorized<br>5. **External installers (Infrastructure)** - external parties contracted to execute the same as the internal installers.<br>6. **Consumers** - Owner of an external asset. They will use the assets that are registered in the system. Example: someone using an electric vehicle. Reporting this vehicle in the blockchain is important for the capacity planning of the energy grid.<br>7. **Energy Web Foundation** - has a developers team building company's application on the top of the EWF's blockchain.<br>8. **Device Manufacturers** - manufactures the device that will be onboarded on the blockchain<br><br>Interviewee **DM04** works frequently with the following stakeholders: **1,2,3,4,7,8.**<br>Interviewee **DM04 has not** provided documents to confirm the mentioned stakeholders. |
| Risks of the blockchain-based systems. | Interviewee **DM04** has identified the following risks:<br>1. **Complexity risks**– The risks that a lot of people will not understand what the system does and how it should work.<br>2. **Unavailability risks**- The risk of the unavailability of the system (caused by bugs or other misfunctions) since the system is not internally controlled but controlled by the EWF.<br>3. **Risk of incorrect asset register** - The risks of not correctly identifying the onboarding assets due to the still use of different systems, causing discrepancies.<br>4. **Risk of malicious installers (external stakeholder)**- The risk that an external party is using the system in a malicious way. |

| | |
|---|---|
| | 5. **Risk of malicious manufacturers (external stakeholder)-** The risk that an external party is using the system in a malicious way.<br>Interviewee **DM04** has the following risks related to his role: **3**<br>Interviewee **DM04 has not** provided documents to confirm the mentioned risks. |
| Risks to the stakeholders of the blockchain-based system. | During the interview **DM04,** the excel-sheet below has been completed to associate the mentioned risks to the mentioned stakeholders, according to the view of the interviewee.<br>Interviewee **DM04** has not provided documents to confirm the mentioned stakeholders' risks. |

| A | B | C | D | E | F |
|---|---|---|---|---|---|
| **Stakeholders / Risks** | **complexity risks** | **unavailability risks** | **risks of incorrect register** | **risks of malicious installers** | **risks of malicious manufacturers** |
| **EWF - builds the blockchain** | | x | | | |
| **inovation department - system business design** | x | x | | | |
| **stedin telecom- related to communication ( router part of telecom)** | x | x | x | x | x |
| **stedin assets management - owner/planning of assets purchases and clife time control / primary users** | x | x | x | x | x |
| **stedin infrastructure and maintenance - internal installer of assets ( scan of devices, idenntification of assets)** | x | x | x | x | x |
| **manufacturer assets - routers/ car/ home batteries** | x | x | | | |
| **installer of assets - external** | x | x | | | |
| **consumers** | x | x | | | |

... interview 2709[redacted]

# Appendix 13.5 - Interview DM05 - In vivo coding

| | |
|---|---|
| Introduction | Interviewee **DM05** is from The Netherlands, is involved with the EWF (energy web foundation, a public blockchain) in 2 projects: Microgrid energy community setting (exchange of energy in the local community) and the Digital Identifier project (Onboarding sensors from devices on the blockchain), has the role of Project Lead/manager at the innovation department, has three years of experience in BBS and works in the energy infrastructure sector. |
| Stakeholders of blockchain-based systems | Interviewee **DM05** has identified the following stakeholders:<br>1. **Residents –** Participants of the energy exchange local communities (microgrids). The blockchain just facilitates their interaction with the user interface. Therefore, the residents have indirect involvement with the blockchain.<br>2. **IT software provider** – Builds the software platform and the forecast systems and algorithms.<br>3. **Innovation department project manager**- Leads the Blockchain project<br>4. **Hardware supplier** - Provides the devices that gather all data, and there is no direct interaction with the blockchain.<br>5. **Municipalities** - interested in how the blockchain project is contributing to their sustainability goals and targets.<br>6. **Asset management department** - Functional owner of the assets, deliver the business rules for the blockchain.<br>7. **Internal Regulatory department** - Blockchain is just a tool for them. They verify blockchain compliance with regulatory requirements.<br>8. **Internal IT department** - Analyze the enterprise architecture to evaluate the future scalability of the blockchain solution within the company enterprise architecture.<br>9. **Telecom department** - Analyses possibilities of onboarding communication devices on the blockchain-related to the improvement of security in communication.<br><br>Interviewee **DM05** works frequently with the following stakeholders: all of them. They need to be informed and involved in the two pilot projects.<br>Interviewee **DM05 has not** provided documents to confirm the mentioned stakeholders and mentioned that the documentation is internal for the company and cannot be shared. |
| Risks of the blockchain-based systems. | Interviewee **DM05** has identified the following risks:<br>1. **Scalability risk**- The risks that the solutions will not be scalable.<br>2. **Standardization risk** - The risks that the various blockchain pilots' projects are not operating together.<br>3. **IoT security breaches** - the risks that the IoT devices can be manipulated without being noticed, and therefore their data will be manipulated.<br>4. **Continuity risks** - the risk that the blockchain service provider stops its activities. It is an external party, and the company has no control over it. |

| | |
|---|---|
| | 5. **Business case risk** - The risk that the blockchain project does not produce any monetary value advantage.<br>Interviewee **DM05** has the following risks related to his role: all the five risks mentioned above.<br>Interviewee **DM05 has not** provided documents to confirm the mentioned risks and mentioned that the documentation is internal for the company and cannot be shared. |
| Risks to the stakeholders of the blockchain-based system. | During the interview **DM05**, the excel-sheet below has been completed to associate the mentioned risks to the mentioned stakeholders, according to the view of the interviewee.<br>Interviewee **DM05 has not** provided documents to confirm the mentioned stakeholders' risks. |

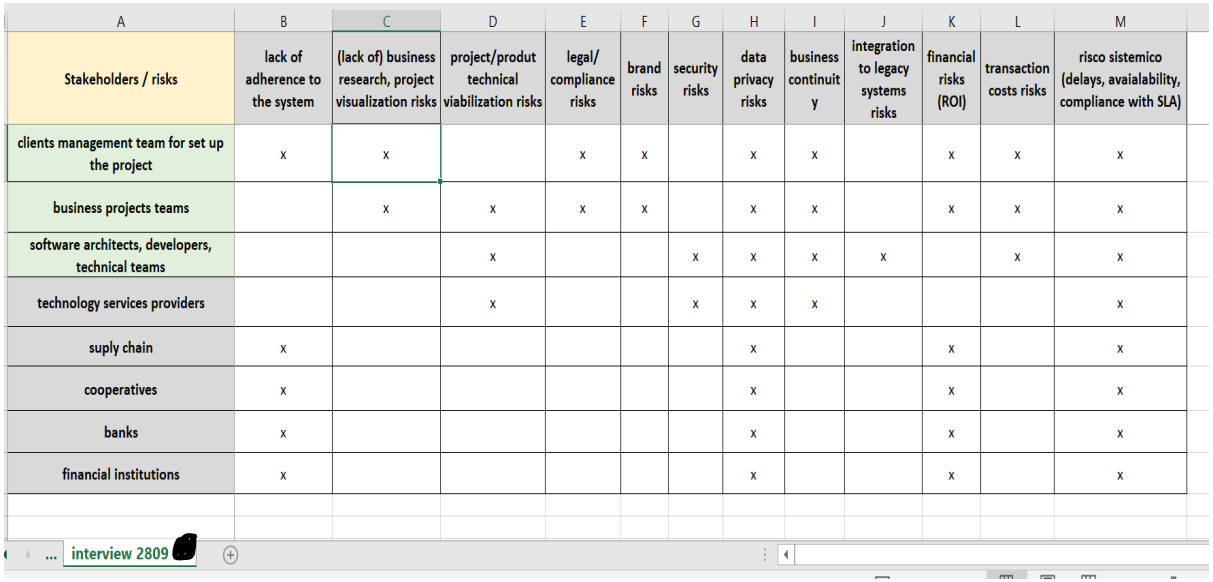
| A | B | C | D | E | F |
|---|---|---|---|---|---|
| **Stakeholders / risks** | **scalability risks** | **standardization risks** | **IoT security breach/leak** | **continuity risks** | **business case risks** |
| **residents - microgrid - na** | | | | | x |
| **IT software provider - development** | x | x | x | | x |
| **Innovation department - project manager -** | x | x | x | x | x |
| **hardware suplier - na** | x | x | x | | x |
| **municipalities** | x | | x | | x |
| **asset management team - business rules** | x | x | x | x | |
| **IT internal - create the environment for the blockchain netowork** | x | x | x | x | |
| **regulatory teams - compliance** | | | | x | x |
| **telecom dept - onboaarding the sim cards ,security improvements** | | x | x | x | |
| | | | | | |

... interview 2809[redacted]

# Appendix 13.6 - Interview DM06 - In vivo coding

| | |
|---|---|
| Introduction | Interviewee **DM06** is from Brazil, is involved with various BBS projects built on Ethereum, has the function of Senior Manager Blockchain Practice, and in the BBS, projects take the role of Product Manager/Business Design Architect (intersection between business and IT), has four years of experience in BBS and works in the Professional Services sector. |
| Stakeholders of blockchain-based systems | Interviewee **DM06** has identified the following stakeholders:<br>1. **Client Management Team** – Management team that contracts and funds the project. They define the business processes, business rules and provide the characteristics of the asset that will be included in the BBS. They are also final responsible for onboarding all the necessary stakeholders from the ecosystem that should be included in the BBS.<br>2. **Business Project Teams** - Build the business design of the project, keep the agile development, agree on definitions for the smart contracts, manage project priorities etc. Project unifications within the participating stakeholder.<br>3. **Software Architects, developers, technical teams** – architects and developers design/build together the technical requirements of the system. The technical teams are related to the normal IT requirements like connection, security requirements, etc.<br>4. **Technology Services Providers** - Third parties that can join depending on what capability they can add, for example, cloud services or a part of the BBS as a service.<br>*5.* **Supply chain** - part of the ecosystem that will use the BBS. They provide the project team with their view of the processes to be used in the system design that should attend to the business needs of all participants.<br>6. ***Cooperatives*** *- part of the ecosystem that will use the BBS. They provide the project* team with their view of the processes to be used in the system design that should attend to the business needs of all participants.<br>7. **Banks** - banks have been mentioned as a stakeholder, but their role in the system has not been discussed. Therefore it is not clear the description of their role in the BBS.<br>8. **Financial institutions** - financial institutions have been mentioned as a stakeholder, but their role in the system has not been discussed. Therefore it is not clear the description of their role in the BBS.<br><br>Interviewee **DM06** works frequently with the following stakeholders: **1,2,3** Client Management Team, Business project teams (for onboarding of the project and definition of the processes and also business lines), and the group of Software Architects, developers, technical teams (for enabling the development phase, definitions and implementation).<br><br>Interviewee **DM06 has not** provided documents to confirm the mentioned stakeholders. DM06 has mentioned that the documents are under a confidentiality agreement and cannot be shared. |

| | |
|---|---|
| Risks of the blockchain-based systems. | Interviewee **DM06** has identified the following risks:<br>1. **Lack of adherence to the system risks** – Risk that the participants of the ecosystem will not see the benefits of adherence to the system.<br>2. **Lack of business research /Project visualization risks** - the risk of not compiling a complete and deep understanding of the business requirements, technical design and assets involved when approving the final design for the project. The risk of not connecting all the dots related to the project.<br>3. **Project technical viability risks** – risks of the project not being technically viable. This risk is present when after the first preliminary analysis of the project proposal from the business stakeholders, the technical teams judge the viability of the project.<br>4. **Legal/compliance risk** - risks in relation to laws and regulatory requirements<br>5. **Brand risks** - risks of possible effects to the brand in case any failure occurs with the project that affects the whole ecosystem.<br>6. **Security risks** - evaluation of levels of access to the system established in the SLA (service level agreement), code security in the smart contracts, possible information leak.<br>7. **Data privacy risks** - risks of exposure of the business data.<br>8. **Business continuity risks** - risks that the continuity of the company and its business may be affected.<br>9. **Integration with existing systems risks** - risks of the various systems not being interconnected with the BBS, creating silos that may create operational issues.<br>10. **Financial Risks (ROI)** - the risk that the initial investment will not produce the expected impact/return.<br>11. **Transaction costs risks** - the risk of increased transaction costs when considered a better performance request from the system.<br>12. **Systemic risks (throughput-time, availability, information leak)** - The risk of spreading various risks along to the various companies participating in the ecosystem.<br><br>Interviewee **DM06** has the following risks related to his role: **2,3,4,5,7,8,10,11,12.**<br>Interviewee **DM06 has not** provided documents to confirm the mentioned risks. DM06 has mentioned that the documents related to risks are sensitive information and besides are under a confidentiality agreement and cannot be shared. |
| Risks to the stakeholders of the blockchain-based system. | During the interview **DM06,** the excel-sheet below has been completed to associate the mentioned risks to the mentioned stakeholders, according to the view of the interviewee.<br>Interviewee **DM06 has not** provided documents to confirm the mentioned stakeholders' risks. DM06 has mentioned that the documents are under a confidentiality agreement and cannot be shared. |



| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Stakeholders / risks | lack of adherence to the system | (lack of) business research, project visualization risks | project/produt technical viabilization risks | legal/ compliance risks | brand risks | security risks | data privacy risks | business continuit y | integration to legacy systems risks | financial risks (ROI) | transaction costs risks | risco sistemico (delays, avaialability, compliance with SLA) |
| clients management team for set up the project | x | x | | x | x | | x | x | | x | x | x |
| business projects teams | | x | x | x | x | | x | x | | x | x | x |
| software architects, developers, technical teams | | | x | | | x | x | x | x | | x | x |
| technology services providers | | | x | | | x | x | x | | | | x |
| suply chain | x | | | | | | x | | | x | | x |
| cooperatives | x | | | | | | x | | | x | | x |
| banks | x | | | | | | x | | | x | | x |
| financial institutions | x | | | | | | x | | | x | | x |

... interview 2809

# Appendix 14 - Stakeholders templates developed: categories, sub-categories, and definitions

| Stakeholders of BBS: Categories & Subcategories | Definitions |
|---|---|
| **S1. Technical stakeholders** | Technical stakeholders are the stakeholders that provide software and/or hardware to the BBS, are involved with coding and designing of BBS, or provide support to the BBS infrastructure. |
| **S1.1 Developers** | Developers are stakeholders that are involved with the coding and designing of the BBS. |
| **S1.2 Vendors** | Vendors are stakeholders that provide software or hardware to the BBS. |
| **S1.3 Facilitators** | Facilitators are stakeholders that contribute to monitoring, maintaining the BBS infrastructure or are responsible for physically installing devices that are related to the BBS infrastructure. |
| **S2. Political stakeholders** | Political stakeholders are involved with the creation of laws, regulations, policies, or standards related to BBS and/or are involved with monitoring the BBS. |
| **S3. Process stakeholders** | Process stakeholders are involved with the creation of the process and development of the BBS project; or involved with the creation, validation and/or analysis of transactions in the BBS. |
| **S3.1 Individual Organizations** | Individual organizations that are involved with the creation and analysis of transactions in the BBS. |
| **S3.2 End users** | End users that are involved with the creation and analysis of transactions in the BBS. |
| **S3.3 Node runners** | Node runners are involved with the creation and/or validation of transactions in the BBS. |
| **S3.4 Project managers** | Project managers design the business processes related to the BBS, keep the overview and control the development of the BBS project. |
| **S4. Investors** | Investors are stakeholders that are involved with contracting and funding the internal BBS projects of an enterprise or are stakeholders involved with making financial investments in the BBS projects. |
| **S4.1 External investors** | External investors are companies or individuals that are making financial investments in the BBS. |
| **S4.2 Internal investors** | Internal investors are high-level management stakeholders within a company that is responsible for contracting and funding the BBS projects within a company. |
| **S5. Social groups** | Social groups are stakeholders interested in the development of the BBS or involved with the creation of BBS and/or research related to BBS. |
| **S6. Other** | Other are stakeholders that have been mentioned during the interviews for which no clear definition has been given or are no-human stakeholders. |

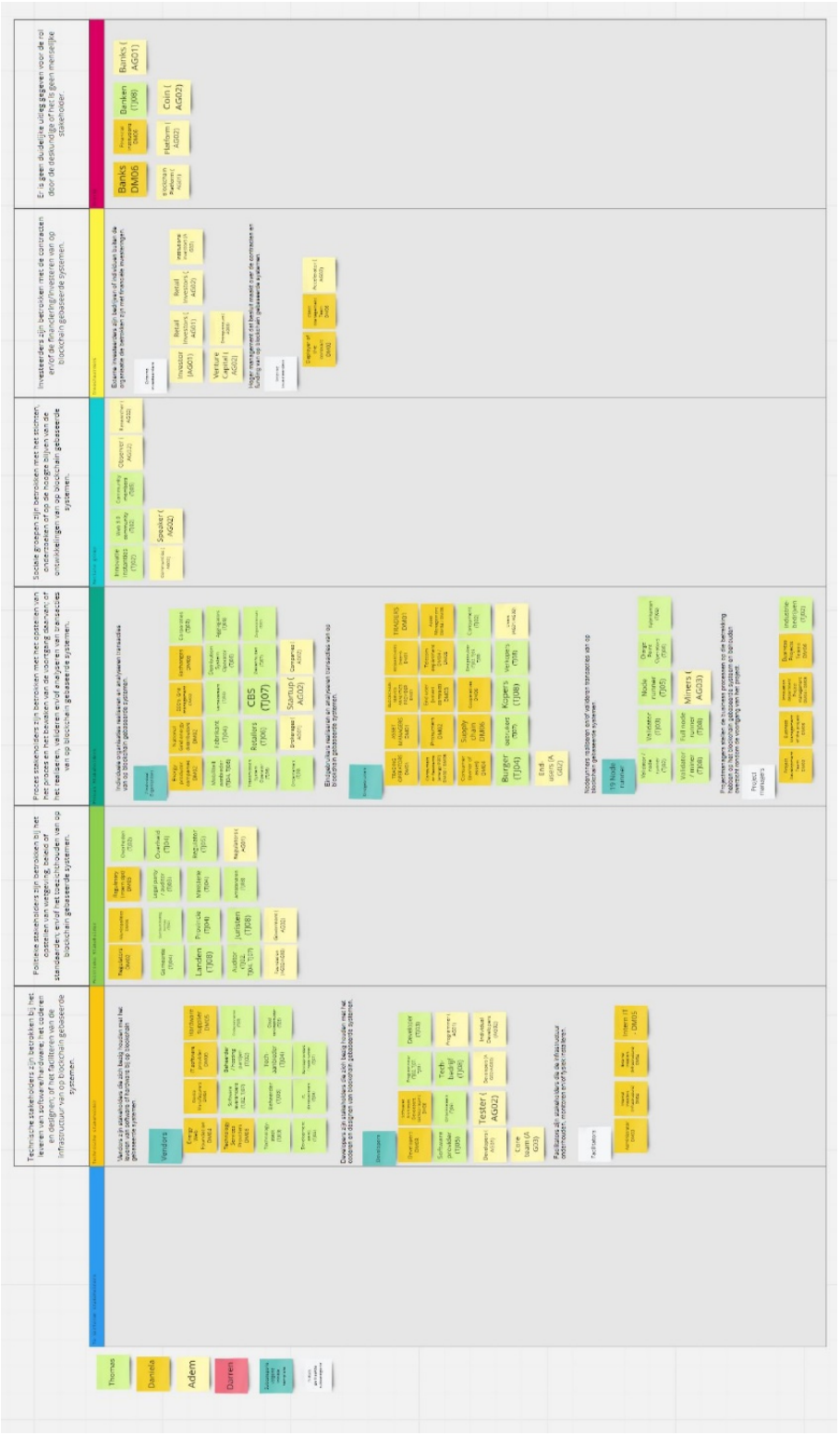
# Appendix 15 - Risks templates developed: categories, sub-categories, and definitions

| Risks of the BBS: Categories & Subcategories | Definitions |
|---|---|
| **R1. Criminal use risks** | Criminal use are the risks that an illicit activity will take place in the BBS in the form of an attack or fraud. |
| **R1.1. Attack risks** | Risk of attack is the risk that an illicit activity will disturb or misuse the functionality of a BBS. |
| **R1.2 Fraud risks** | Risk of fraud are the risks that criminals will manipulate, steal, or misuse data, information, passwords, or assets from BBS's users. |
| **R2. Technical risks** | Technical risks are the risks of weaknesses in the code, infrastructure, or governance of the BBS. |
| **R2.1 Coding risks** | Risks of insufficient coding or the existence of bugs in the code of the BBS. |
| **R2.2 Infrastructure risks** | Infrastructure risks are the risks that the performance and use of the BBS will deviate from the expectations. |
| **R2.3 Governance risks** | Governance risks are the risk that consensus may not be achieved about decisions related to security, compliance, current and future applications of BBS or that such decisions are made by a small group of developers. |
| **R3. Privacy risks** | Privacy risks represent the loss of control related to how private information is processed and linked to a person's identity on the BBS. |
| **R4. Legal risks** | Legal risks are the risks related to the uncertainties about laws, regulations, and executions of BBS. |
| **R5. Human risks** | Human risks are the risks related to misunderstanding, lack of knowledge and errors using BBS. |
| **R6. Financial risks** | Financial risks are the risk related to the volatility in a transaction and operational costs of the BBS. |
| **R7. Business case risks** | Business case risks are related to the risks to the future adherence to the system and risks to the company strategic goals associated with the BBS. |
| **R7.1 Strategic risks** | Strategic risks are the risks that may affect the business and business goals that are related to the BBS. |
| **R7.2 Lack of adherence to the system risks** | Lack of adherence risks are risks that may influence the willingness to participate in the BBS. |
| **R8. Economic risks** | Economic risks are risks related to the influence of the BBS on a country's economic policy. |

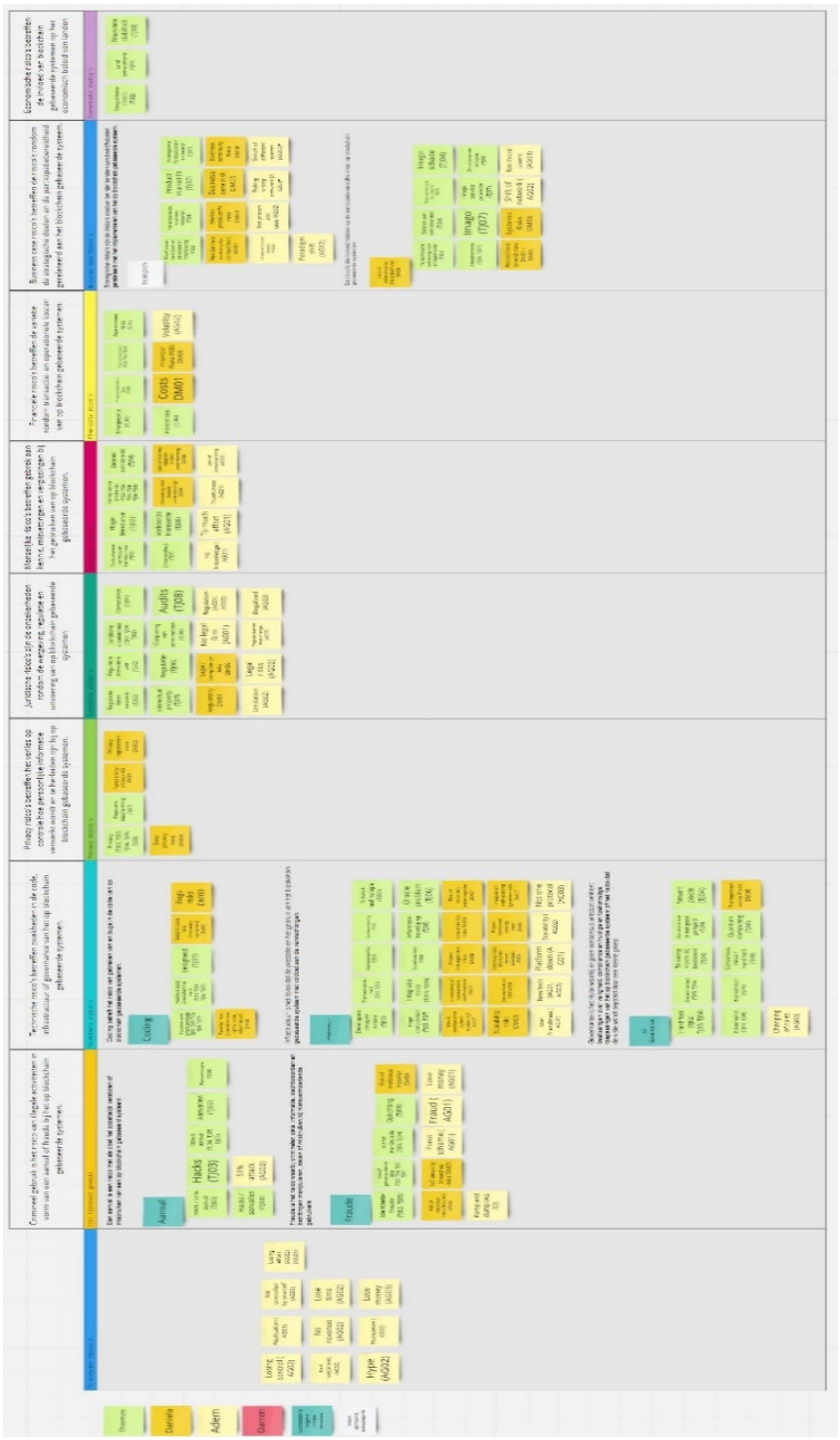
# Appendix 16- Miro board templates print screen

The original Miro boards are presented below (For visualization of the Miro boards used). However, due to its size and lack of legibility, the print screen presented below, with the information related to the categories, sub-categories and definitions of the templates created, are translated into English and presented in tables that have been included in appendices 14 and 15.

1. Stakeholder's template developed on Miro board



2. Risk's template developed on Miro board



## Attachment 1- Word files - Interview transcripts


DM01 interview DM 14sep transcript.docx


DM02 interview RH 20sep transcript.docx


DM03 interview KFB 24sep transcript.docx


DM04 interview SH 27sep transcript.docx


DM05 interview AZ 28sep transcript.docx


DM06 interview FX 28sep transcript.docx

## Attachment 2- Excel file - RQ3 Matrix: risks to the stakeholders


attachment 2 RQ3 risks to stakeholders r