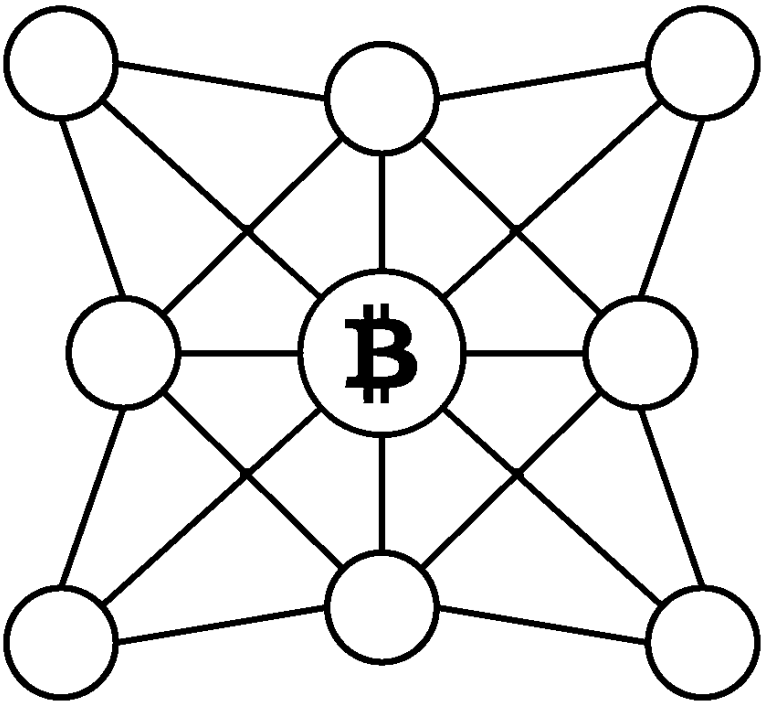
Building a better working world

TILBURG UNIVERSITY

School of Economics and Management

Blockchain Audit & Assurance
– *Towards an Audit Standard for the Consortium Blockchain*



Kazem Nosrati

Master Thesis

MSc Information Management

25 July 2022

Blockchain Audit & Assurance

- Towards an Audit Standard for the Consortium Blockchain

Author

Kazem Nosrati

SNR: 2056486

ANR: 214623

Information Management

k.nosrati@tilburguniversity.edu

Internship company

EY (Ernst & Young)

Boompjes 258, 3011 XZ, Rotterdam,

Company supervisor: Ashish Gupta

University

Tilburg University

TiSEM (Tilburg School of Economics and Management)

Warandelaan 2, 5037 AB, Tilburg

Supervisor: dr. Joris Hulstijn

Second reader: dr. Martin Smits

Preface

In the name of God, the *Most Gracious*, the *Most Merciful*,

In front of you is my thesis which I completed as part of my graduation from Tilburg University's Faculty of Tilburg School of Economics, its Information Management program. I did my research at EY in Rotterdam, the Netherlands, between the 1st of March till the 16th of July 2022.

It was a difficult task to undertake. I would not be able to achieve this alone without all my incredible support. Therefore, I would like to thank my internship supervisor Ashish Gupta for sharing his knowledge and the discipline that comes with the field of IT audit. I would also like to thank my study supervisor Joris Hulstijn for his academic guidance and support during this process. Furthermore, I would like to thank my colleagues at EY for their willingness to cooperate and the respondent from NEN and NOREA for their congress in May. I would also like to credit the respondents from R3, Hyperledger Foundation, and B3i, who took the time to give off an interview.

I have also received wise advice from my friends and family, especially my wife, Melina. They have morally supported me during the execution of my research. Most importantly, all praise be to God, which, without His help, I wouldn't be where I am right now.

I wish you a pleasant reading.

Kazem Nosrati

Rotterdam, 25 July 2022

Management Summary

In response to the need for trust, firms like EY are planning and preparing their operating business line of assurance for blockchain called 'Blockchain Assurance.' This need for trust is due to the rise of blockchain services, and the necessity for assurance comes from blockchain scandals in the past. To prevent these risks, good governance could be a solution. However, due to the decentralized nature of blockchain, it can be rigid to have appropriate governance. Governance should describe the ways that participants interact and make decisions and that it is crucial to organize governance early on to prevent the consortium from failing. Nonetheless, is still no auditing standards for consortium blockchain to this day which makes it necessary to develop new standards regarding auditing blockchain.

In order to answer the research question: *"How should an IT auditor audit a consortium blockchain(s)?"* this research aims to take the first step towards improving the auditability of consortium blockchain by making available a concept principle-based IT audit standard that satisfies auditability, control, and governability requirements to help IT auditors audit consortium blockchain(s) To help understand the topic, based on the literature review research, the ABC model is created to give a holistic view of stakeholders and the relationship between the investors or shareholders (principal/trustor), the consortium blockchain client (agent/trustee), and the external auditor (control mechanism) of the consortium blockchain.

In order to answer the research question, a design science research was conducted where 12 interviews were held divided into three phases: requirements (five), design (three), evaluation (three), and communication (one) with blockchain experts, IT auditors, consortium blockchain providers, and Standards Development Organizations (SDO). Respondents were chosen based on their expertise in either of the subject's audit & assurance and/or blockchain.

Based on the findings of the consortium blockchain providers, it was found that off-chain governance is more of an issue than on-chain governance, which aligned with the findings from the literature review and was scoped for the CBAC (Consortium Blockchain Audit Control) Framework that was developed and evaluated in the evaluation phase.

Based on this CBAC Framework, it is recommended to educate IT auditors on the topic of blockchain to enhance their professional judgment in using the CBAC Framework.

Table of Contents

Preface i
Management Summary ii
List of Tables and Figures vi
1 Introduction 1
1.1 Problem Indication 1
1.2 Problem Statement 2
1.2.1 Academic Relevance 3
1.2.2 Managerial Relevance 4
1.3 Research Goal 4
1.4 Research Scope 4
1.5 Research Question 5
1.6 Thesis Structure 5
2 Literature Review 6
2.1 Blockchain 7
2.1.1 What is blockchain 7
2.1.2 Blockchain Components 8
2.1.3 Types of Blockchain 10
2.1.4 On-chain and off-chain 12
2.2 Smart (Business) Network 13
2.2.1 Performance of the Network 15
2.3 Extended Strategic Alignment Model 17
2.4 Network Governance 20
2.5 Model of Trust 23
2.6 Agency Theory 24
2.6.1 Agency Theory in Audit 26
2.7 Audit & Assurance 27
2.7.1 Assurance 27
2.7.2 Audit 28
2.7.3 IT Audit Procedures 28
2.7.4 The Role & Responsibility of the Auditor 28
2.7.5 Principle-based vs Rule-based norms 29
3 Theoretical Framework 30
3.1 ABC Model 30

4 Methodology 33
4.1 Research Approach 33
4.2 Research Method 33
4.3 Research Paradigm 33
4.4 Research Framework 34
4.5 Research Design 35
4.5.1 Research Type 35
4.5.2 Research Strategy 35
4.6 Research Process 38
4.6.1 Research Setting 38
4.6.2 Working Method 39
5 CB Findings 43
5.1 Off-chain Focused 43
5.2 Governance Structure Consortium Blockchain 44
5.3 The Accountable Client Entity 47
6 Design Artifact 48
6.1 Background Information 48
6.2 Requirements 49
6.3 Design 50
6.4 Consortium Blockchain Standard 52
6.4.1 Intro 52
6.4.2 Consortium Blockchain Roles 52
6.4.3 CBAC Framework 55
7 Evaluation 61
7.1 Evaluation 61
8 Communication 65
8.1 Conclusion 65
8.2 Recommendation 67
8.3 Contribution to Theory and Practice 67
8.4 Limitations & Future Research 67
References 69
Appendices 72
Appendix A: Interview Transcripts 72
Respondent 1: Employee from NEN 72

Respondent 2: Blockchain expert at EY (I) 75
Respondent 3: Employee at Corda Network of R3 79
Respondent 4: Employee at Hyperledger Foundation 89
Respondent 5: Employee at B3i 98
Respondent 6: Blockchain Expert at EY (II) 106
Respondent 7: Blockchain Expert at EY (III) 114
Respondent 8: Blockchain Expert at EY (IV) 118
Respondent 9: IT auditor at EY (II) 125
Respondent 10: IT auditor at EY (III) 131
Respondent 11: IT auditor at EY (IV) 136
Respondent 12: Blockchain expert at EY (same person as R2) 141
Appendix B: Profiles 147
Audit Firm Profile 147
Consortium Profiles 147
Profile 1: R3 149
Profile 2: Hyperledger Foundation 150
Profile 3: B3i 151
Appendix C: Consortium Nodes 152
R3 152
Hyperledger Foundation 159
B3i 167
Appendix D: Code Scheme 168
Code Scheme Overview Version 168
Code Scheme Detailed Version 169
Appendix E: NOREA Congress 191

List of Tables and Figures

Table 1 11
Table 2 15
Table 3 18
Table 4 22
Table 5 29
Table 6 39
Table 7 41
Table 8 41
Table 9 50
Table 10 53
Table 11 56
Table 12 77
Table 13 147
Table 14 147
Table 15 148
Table 16 148
Table 17 152
Table 18 159
Table 19 167
Table 20 169

Figure 1 6
Figure 2 7
Figure 3 8
Figure 4 9
Figure 5 15
Figure 6 16
Figure 7 17
Figure 8 19
Figure 9 21
Figure 10 23
Figure 11 24
Figure 12 25
Figure 13 27
Figure 14 32
Figure 15 34
Figure 16 46
Figure 17 46
Figure 18 54
Figure 19 63
Figure 20 66
Figure 21 74
Figure 22 83
Figure 23 84

Figure 24 86
Figure 25 87
Figure 26 95
Figure 27 99
Figure 28 106
Figure 29 107
Figure 30 133
Figure 31 168

1 Introduction

This chapter explains the research topic by defining the context in which it is conducted, as well as the problem indication, problem statement, research goal, research scope, research questions, research technique, the academic and practical relevance of the research, and the structure of this thesis report.

1.1 Problem Indication

Due to high growth in blockchain service, a new market is likely unfolding for the assurance business called blockchain assurance which focuses on auditing blockchain technology, its service providers, or user entities. With more and more organizations emerging involved in the use and provision of blockchain technology, a need for trust arises, where user entities need confidence in the service entities that are provided via a formal audit by a trusted third party. Such trusted third audit parties are companies like the Big Four accounting firms. In response to the need for trust, firms like EY are planning and preparing their operating business line of assurance for blockchain called 'Blockchain Assurance' (Halterman et al., 2021).

The necessity for assurance comes from blockchain scandals in the past, especially in the territory of cryptocurrency. A recent example is TerraUSD, a stablecoin designed to be coupled with the value of $1 per coin. TerraUSD was positioned as a safe haven from bitcoins' high volatility. However, it slipped below $1 earlier this month, trading even below 20 cents (Browne & Sigalos, 2022; Hern, 2022). In addition, there are still no auditing standards for blockchain to this day (Gauthier & Brender, 2021) which makes it necessary to develop new standards regarding auditing blockchain (Dai & Vasarhelyi, 2017; Nóbrega et al., 2021).

Especially in the case of a consortium blockchain. A consortium blockchain is a type of blockchain that is a private permissioned network formed when a group of people works together to achieve a shared goal, and thus only members can access the transactions (Nathan & Jacobs, 2020; Zheng et al., 2017). consortium blockchain may offer more security, anonymity, and quicker transaction confirmations than a public blockchain since all members are known to one other. However, furthermore, insight needs to be obtained regarding how the consortium blockchain should be governed. Likewise, institutions have expressed worry about the lack of attention given to governance problems in blockchains. Oversight and governance procedures are needed in order to ensure the correct functioning of the system by providing incentives and determining culpability. An example of this is the issue of establishing explicit trust boundaries

when integrating ledgers with the 'real world,' such as determining who is responsible for ensuring that new data such as the attributes of a physical item are accurately recorded (Hileman & Rauchs, 2017).

This research requires information by analyzing existing IT audit standards and a set of consortium blockchain providers that need to be interviewed and inquired about their expertise. Based on the audit firm requirements, an artifact is made in the form of a conceptual principle-based IT audit standard specific to consortium blockchain. This concept standard will contribute to further developments of standards and their practical usage within EY.

1.2 Problem Statement

IT auditing as a discipline has existed for more than forty years and has seen much growth in recent years, indicating it is a mature field with plenty of room for growth (Fijneman, 2006). IT audit is the auditing of IT which includes information systems, networks, and databases IT audit is the auditing of IT, which includes information systems, networks, and databases. IT audits look at an information system's controls to see if it complies with internal control policies and external laws and regulations in order to protect the company's assets (Romney & Steinbart, 2015). As an IT-Auditor, the profession is to assess a company's internal controls to ensure processes and systems run accurately and efficiently, remain secure and meet compliance regulations (Dutta et al., 2022). Moreover, IT audit helps automation to minimize risk and enhance operational efficiency (Dzuranin & Mălăescu, 2016). The IT auditor does the job in aid by a suitable standard. Standardization is necessary to facilitate straight-through processing and interoperability across systems and participants, as well as accurate data interpretation (Le Borne et al., 2017).

However, due to the fast-changing technology and increasing regulatory requirements, IT auditing is facing auditability issues due to a lack of standards (Dutta et al., 2022; Dzuranin & Mălăescu, 2016; Gauthier & Brender, 2021). An example of one of these technologies is blockchain, which is a catchall term for multiple key components than can work together like: distributed ledger technology (DLT), peer-to-peer (P2P) network, cryptography, consensus mechanism, and smart contract. Blockchain is a type of distributed ledger composed of a chain of cryptographically-linked blocks containing batched transactions, which generally broadcasts all data to all participants in the network (Hileman & Rauchs, 2017). So auditing blockchain is checking the different components. Things get more difficult in the case of consortium blockchains, where a group of

entities works together with a common goal. Due to the decentralized nature of blockchain, it can be rigid in having appropriate governance. Nathan and Jacobs (2020) state in their paper that governance should describe the ways that participants interact and make decisions and that it is crucial to organize governance early on to prevent the consortium from failing (e.g., due to conflict of interest between members of the consortium). Moreover, Provan and Kenis (2008) also state that according to most studies on organizational networks, there is little to no discussion of governance due to the absence of legality of the network as a legal entity. Therefore the legal importance of governance is not available.

In traditional auditing, auditors have audit standards to check controls to see if it complies with the internal & external policies. However, blockchain organizations, for example, have built controls into 'smart contracts. Smart Contracts make the design transparent for those who can read the code (e.g., developers) (Weigand et al., 2020). Nevertheless, there are still risks associated with control deficiency within the blockchain organization. For example, the failure of an access control mechanism may result in unauthorized transactions or disclosures of confidential information, and system requirements may not comply with laws and regulations (AICPA, 2020) or questions like which firms can participate in the blockchain? (Smits et al., 2018). Henceforward, blockchain standardization is needed to build trust between different entities and to make distributed ledgers interoperable, and the information recorded on the ledger conforms to market rules and practices (Gauthier & Brender, 2021; Le Borne et al., 2017). However, the assurance of blockchain remains undeveloped, creating demands for standards (Dai & Vasarhelyi, 2017; Nóbrega et al., 2021).

1.2.1 **Academic Relevance**

There have been no previous studies that particularly show audit standards for auditing blockchain, especially in the case of a consortium blockchain. Although Gauthier and Brender did similar research in 2021, the limitation of their study is that their research only focuses on standards for Swiss external auditors on blockchain for specific individual entities (nodes). However, that same research suggested that future research can be done in contribution to blockchain-exclusive IT auditing standards for the auditing practice, as this is still an understudied area. Therefore, this research builds on current literature in the field of audit & assurance and blockchain technology and contributes to the IT audit discipline hence contributing also to the field of Information Management.

1.2.2 Managerial Relevance

The Big 4 firms are exploring and exploiting blockchain technology and how they can provide value to their clients who are in the blockchain market by providing services like assurance so that blockchain providers can assure their customers. The findings of this research may be used further develop the model and contribute to the EY business and complement their existing operating business of IT auditing.

1.3 Research Goal

The research goal is formulated using the template by Wieringa (2014). The research goal is to:

Improve	the auditability of consortium blockchain
by	making available a concept principle-based IT audit standard
that satisfies	auditability, control, and governability requirements
in order to	help IT auditors audit consortium blockchain(s).

1.4 Research Scope

Due to the many audit standards and a short thesis period of three months, the scope of the thesis is limited to building a concept standard that is based on the ISAE 3000. The ISAE 3000 is a standard used for SOC 2 reporting that is for assurance over non-financial controls examined against each of the TSCs that have to be met by implementing the internal controls according to the predefined requirements (EY, n.d.). Furthermore, the research from the audit perspective is limited to only EY and does not take into consideration other accounting firms, e.g., Big Four companies like Deloitte, PwC, and KPMG. The reason is that first of all, the standard methodology for auditing is international and, therefore, for all audit firms, the same. Secondly, also due to limited time, it is more feasible to have interviews within EY.

This study focuses on a concept principle-based IT audit standard for auditing a consortium blockchain. In the case of blockchain, this research will focus on consortium blockchains, which is a partnership of limited organizations with the same goal or objectives. This study gives importance to how governance should be shaped due to the lack of client accountability during the audit process. This research does not focus on the technicalities of blockchain, nor will it provide the how-to audit procedures.

1.5 Research Question

To explore the research topic mentioned earlier the following main research question is formulated with three supporting sub questions.

Main question:

- How should an IT auditor audit a consortium blockchain(s)?

Sub questions:

1. What governance structure would be suitable for a consortium blockchain?
2. Who should be the accountable client entity in the consortium blockchain regarding the audit process?
3. What norm controls should be implemented in a consortium blockchain?

1.6 Thesis Structure

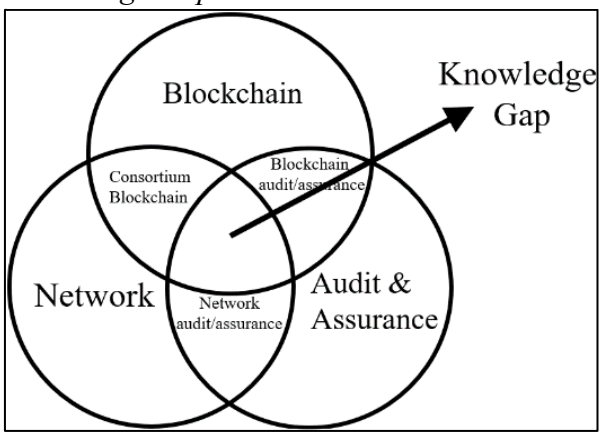
This thesis consists of eight chapters. These chapters are as follows. First chapter one gives background in by stating the problem indication, problem statement, academic & managerial relevance, research goal, research scope, and the research questions. Next, chapter two consists of a thorough literature study of the topics blockchain, smart business networks, extended strategic alignment, network governance, agency theory, and (IT)audit & assurance. Then, chapter three introduces the ABC model that is set as the theoretical framework. Then, chapter four explains the methodology of this research by illustrating the research approach, method, paradigm, framework, design, and process. Chapter six, an artifact, is designed based on the input of literature and interviews. Afterward, in chapter seven, the artifact is then evaluated and adjusted according to the input received from auditors. Finally, in chapter eight, the research is concluded by answering the research question, giving a recommendation and contribution to theory & practice, limitations to the research, and indicating future research.

2 Literature Review

This chapter includes a substantive literature review to get an in-depth view and understanding of concepts, models, and theory around network, blockchain, and audit & assurance to help answer the research questions of this thesis. To get a picture, figure 1 shows a Venn diagram that consists of three distinct topics, blockchain, network, and audit & assurance, crossed with each other to form the knowledge gap of this research. That is consortium blockchain audit & assurance. This chapter aims to get an understanding of consortium blockchain (as a whole network & system) by first introducing network-related theory. Whereby audit & assurance-related theory helps to understand how consortium blockchain(s) could possibly be audited. The literature review consists of two parts. First, this chapter will describe each theory or topic. Then it will apply the theory or topic (either in the form of models or a description) in the context of consortium blockchain.

Figure 1

Knowledge Gap



First, the chapter goes into what blockchain is, the types of technology, and what types of blockchain there are. Next, the research describes smart business networks to understand why networks are developed and the three layers of business to understand the formation of complicated interactions between network nodes, the types of couplings, and the advantages and disadvantages of networks. Then, the extended strategic alignment model is discussed to understand the inter-organizational alignment between businesses. After, the discussion turns to network governance to comprehend how a network is governed and what types of governance exist. In addition, Mayer's trust model defines trust in the network, which is defined as the degree to which trustor's (e.g., investors, shareholders) trust the network based on the network's ability, benevolence, and integrity.

Afterward, the agency theory is discussed to explain and resolve concerns in the connection between entities (principals) that lawfully designate people to act on their behalf (agents). Involving a third party, such as the auditor, is one of the primary means of reassuring the

principal organization. Based on this, this study will briefly address audit and assurance and the significance of delivering confidence to the network users of the audited party who require it.

Finally, This all breaks down to a summarizing and holistic model based on the discussed theories and models to give an understanding of auditing consortium blockchains.

2.1 Blockchain

This chapter focuses on what blockchain is, what type of blockchains there are, and what gaps there are that explain the importance of this study.

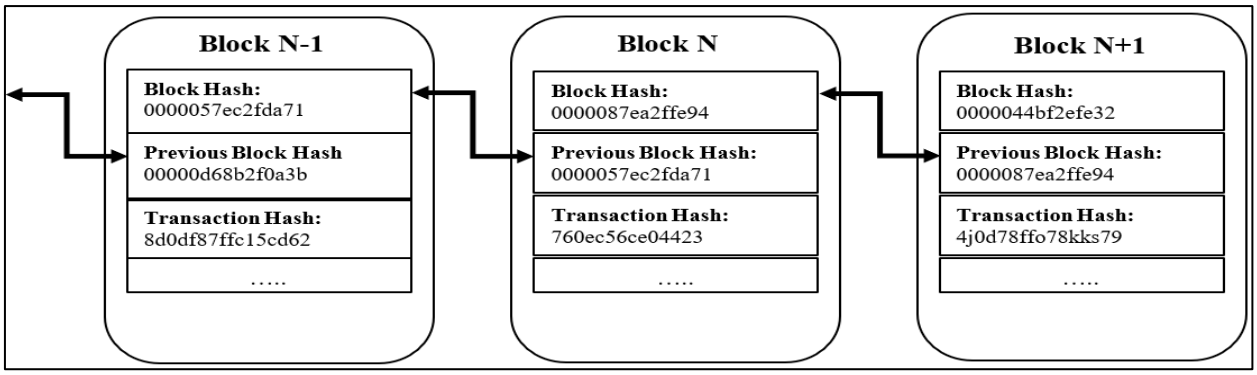
2.1.1 What is blockchain

Hileman and Rauchs (2017) define blockchain as "*a type of distributed ledger that is composed of a chain of cryptographically-linked blocks containing batched transactions; generally broadcasts all data to all participants in the network.".*

Blockchain, as the name suggests, consists of blocks of transactional records that form a chain when the hash digest of the preceding block's header is included in each subsequent block. This hashing allows for the detection and rejection of tampered blocks. The hash of a previously published block would be altered if any changes were made. Because they incorporate the preceding block's hash, all future blocks would have different hashes as a result (Yaga et al., 2019; Zheng et al., 2017). See figure 2. By cutting away the middlemen and using a blockchain as a "trust agent," it is possible to facilitate peer-to-peer asset transfers and gain the advantages such as lower transaction fees and faster transactions.

Figure 2

Transaction Chain of Blocks



Note. From screenshot from workshop EY Europe West Conference 2022: Blockchain Explained.

2.1.2 Blockchain Components

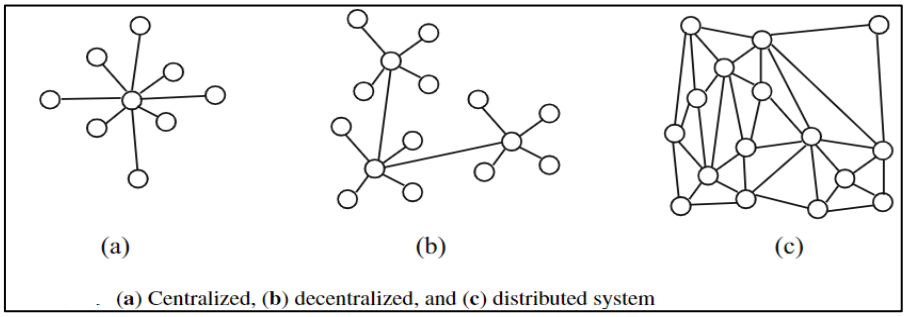
Hileman and Rauchs (2017) state that a blockchain mostly has the following five components:

DLT

A distributed ledger is a shared database that stores the same data across multiple locations (nodes) instead of one central database (node). A node is a common term for each of these computers. It is possible to see a distributed ledger as a single datasheet held on several distributed nodes in a decentralized manner where storing, disseminating, and transmitting data between users across private or public distributed computer systems are done (Liu et al., 2020). Figure 3 visualizes the difference between central, decentral and distributed systems.

Figure 3

DLT Configurations



Note. From *Intelligent Internet of Things From Device to Fog and Cloud* (p. 394), by F.Firouzi, K.Chakrabarty, and S.Nassif, 2020, Springer (https://link.springer.com/book/10.1007/978-3-030-30367-9). Copyright 2020 by Springer Nature Switzerland AG 2020.

P2P Network

A Peer-to-peer (P2P) network is a decentralized network created when two or more participants (or nodes) connect and share their digital resources like processing power, storage capacity, and network connection capacity enabling the facilitation of transactions without an intermediary. A peer-to-peer network can also be considered a distributed network where resources are immediately accessible by other peers without going through intermediate organizations. Members of a network like this are both suppliers and consumers of digital assets (Schollmeier, 2001). Schollmeier (2001) furthermore divides P2P networks as those with a central node (Hybrid) and those without a central node (Pure). Kellerer (1998) defines a “Pure” P2P network as a distributed network architecture with a Peer-to-Peer network, firstly without a central node, and secondly, if any important node is removed from the network, the network would not suffer any loss of network service. Kellerer (1998) defines the “Hybrid” P2P network

as a distributed network architecture where a central entity is necessary to provide parts of the offered network services. See figure 3 configuration (c).

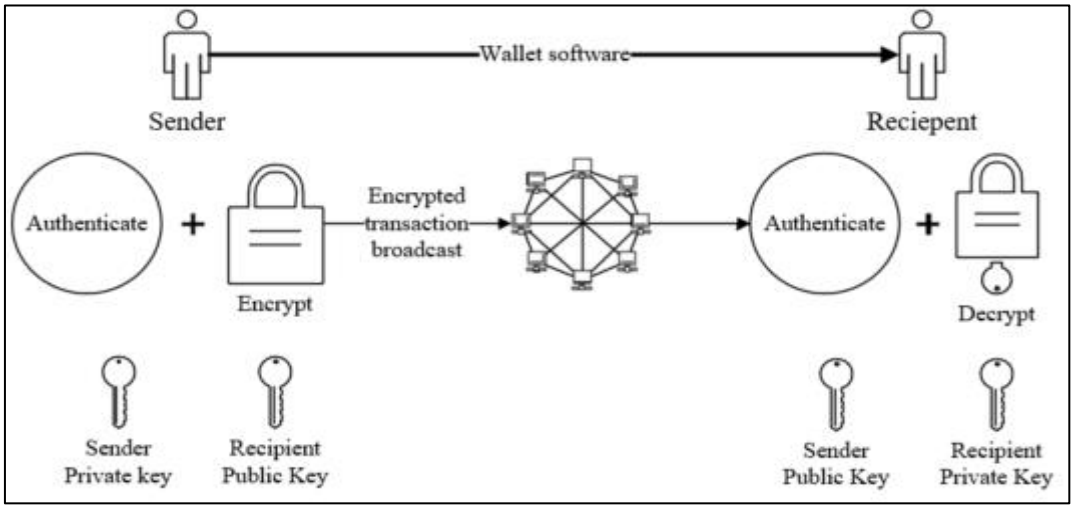
Cryptography

Cryptography is a method of protecting information and communications using codes so that only those for whom the information is intended can read and process it. Kessler (2003) discusses three types of cryptographic algorithms:

- Private Key Cryptography: Using a single key for encryption and decryption.
- Public Key Cryptography: Using one key for encryption and one for decryption.
- Hash Functions: Using mathematical modification to "encrypt" information that cannot be decrypted.

Figure 4

Transaction on the Blockchain



Note. Adapted from "Blockchain Bronze Training," by EY, 2022.

In a blockchain, the Public KC algorithm and the hash function are used. The Public KC consists of two separate keys: public and private keys. Users can share their public key (which can be seen as an email address) with others. The other key is the private key, which is never shared with anyone. For example, if person (A) wishes to share data with person (B), (A) uses the public key of (B). Decryption is performed by (B) using their private key. Suppose that (A) encrypts some plaintext using their private key; when (B) decrypts using the public key of (A), (B) knows that (A) delivered the message, and (A) cannot deny having transmitted the message. This technique may also be used to find out who sent a message (Kessler, 2003).

The integrity of a file may be determined via the use of hash functions (Kessler, 2003). Hash functions are one-way encryption and require no key. Rather, a hash value of a defined length is generated from the plaintext, making it impossible to decode the contents or determine the length of the plaintext. To verify that a file has not been tampered with by a virus, for example, hash techniques are often utilized. Many operating systems also use hash algorithms to secure passwords.

Consensus Mechanism

A consensus mechanism in blockchains achieves an agreement on a single state of all transactions in a bitcoin blockchain. There are many different types of consensus mechanisms. Therefore, Alsunaidi and Alhaidari (2019)classify them into two categories of consensus protocols: proof-based and vote-based.

Proof-based protocols function on asynchronous communication networks suitable for public applications where any user or limited nodes may participate. Common ones are PoW and PoS (Rebello et al., 2020).

Vote-based, on the other hand, does not begin with the identification of participating nodes in verification until after all nodes have been identified. To determine whether or not to add a new block to the chain, the node will connect with other nodes (Alsunaidi & Alhaidari, 2019). In addition, the transaction will be verified by all network nodes.

Smart Contract

Smart contracts are self-executing software codes that automatically perform functions on a decentralized blockchain network and let untrusted parties trade without a central authority. To ensure smart contracts are implemented correctly, consensus protocols are implemented. If a trigger condition is met, the contracts may be programmed to carry out any pre-defined actions. The most common platform for generating smart contracts is Ethereum, where smart contracts are developed and run on the Ethereum Virtual Machine (EVM) (Wang et al., 2018).

2.1.3 Types of Blockchain

Blockchain can be classified into three categories: public, private, and consortium (Zheng et al., 2017).

Public Blockchain

Everyone can participate in the consensus process in a public blockchain since all records are made available to the general public. A well know example is Bitcoin, founded by pseudonymous person(s) Satoshi Nakamoto (Zheng et al., 2017).

Private Blockchain

In a private blockchain, the nodes from one organization are allowed to join the consensus process, and therefore, private blockchains are considered centrally controlled networks since they are owned and operated by a single entity (Zheng et al., 2017).

Consortium Blockchain

A consortium blockchain is a type of blockchain that is private, and only members can access the transaction (Zheng et al., 2017). Consortiums are formed when a group of people work together to achieve a shared commercial goal and are more secure than public blockchains since the consortium members are known to other participants. Furthermore, they provide a safe and trustworthy environment for cooperation where participants in the consortium evaluate and vote on whether or not certain businesses should be allowed to join the network. Members may then assign responsibilities for carrying out the group's business goals after they have been admitted as members. Participation in a consortium network can be facilitated by using private blockchains such as Corda, B3i Fluidity, and Hyperledger Fabric, which may transmit sensitive data between members. As a result, consortium members can achieve business objectives they could not have achieved on their own. The Know Your Customer (KYC) procedure exemplifies this synergy (Nathan & Jacobs, 2020). See table 1 for an overview.

Table 1

Comparisons Among Public Blockchain, Consortium Blockchain and Private Blockchain

Property	Public blockchain	Private blockchain	Consortium blockchain
Consensus decision	All miners	One firm	Selected nodes (network governance board)
Read permission	Public	Private (could be public)	Network members only (could be public)
Immutability	Nearly impossible to tamper due to large number of participants	Could be tampered due to limited number of participants	Could be tampered due to limited number of participants
Efficiency	Low	High	High
Centralized	No	Yes	Partial
Consensus process	Permissionless	Permissioned	Permissioned

Note. Adapted from "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," by Z.Zheng, S.Xie, H.Dai, X.Chen, and H.Wang, 2017, *2017 IEEE International*

Congress on Big Data (BigData Congress),
p. 559. (https://doi.org/10.1109/bigdatacongress.2017.85) Copyright 2017 by IEEE.

According to Genesis Block (2020), consortium blockchains can be further divided into three types:

- **Business-Focused:** Consortiums that focus on particular business issues, such as banking, supply chain, and healthcare, and provide services for commercial use solely instead of providing them as open-source platforms (e.g., B3i)
- **Technology-Focused:** Consortium that provides open-source software and reusable blockchain platforms (e.g., Hyperledger).
- **Dual-Focused:** Consortiums that do both business and technology. Besides commercial items, they provide an open-source platform that might be used for any solution (e.g., R3).

2.1.4 On-chain and off-chain

On-chain

On-chain refers to storing all types of data onto transactions recorded on the blockchain that is publicly accessible (Hepp et al., 2018; Zheng et al., 2021). On-chain governance describes rules and procedures included in the blockchain's underlying technology. Participant interactions in this governance model can only be governed by rules inherent in the underlying blockchain code, which dictate the laws of interaction between members. Since the rules are directly written into the system, the system is responsible for enforcing the rules, and therefore, on-chain governance cannot be readily evaded by anyone. Since no one person or group can exert their authority over a big group, on-chain governance seems to be the most desirable style for blockchain-based systems (Reijers et al., 2021).

Off-chain

Off-chain can be described as storing information outside the blockchain in various forms. Off-chain could be essential when an organization does not want to make sensitive information public or available to other participants. Also, the amount of data on the blockchain may exceed its capacity (Hepp et al., 2018). Outside authorities can intervene in the blockchain protocol via off-chain governance. Off-chain governance, on the other hand, places the power of decision-making in the hands of the people rather than the code itself. Off-chain governance raises the

issue of individual sovereignty by strong individuals dominating decision-making processes (Reijers et al., 2021).

Key elements

Hileman and Rauchs (2017) state that on-chain data storage is decreasing; 70% of DLT network operators only save hashes that refer to off-chain data. Moreover, third parties are often necessary to provide connections between distributed ledgers and the physical world. Furthermore, state according to on-chain governance, no one or group of people should be able to impose their will on others and individual sovereignty should be diminished throughout the decision-making process. Nonetheless, by employing off-chain processes to usurp on-chain governance, blockchain-based systems become more susceptible than ever to private interests rising to dominance. During the state of exception, autonomy establishes itself using off-chain means rather than following the 'rule of code' in a formal sense.

Moreover, according to Williams (2020), it appears that once a transaction is posted to the blockchain, it is considered genuine even if the human actors on the blockchain have validated it incorrectly. The blockchain does not allow for eradication; therefore, human stakeholders cannot interfere. In other words, the information itself needs to be checked for correction before being placed on the blockchain, not per se the blockchain itself. Moreover, people are still in control instead of full automation. This indicates that monitoring is more needed on the off-chain side instead of the on-chain.

2.2 Smart (Business) Network

This study takes the definition by Provan et al. (2007); Provan and Kenis (2008) state that networks are *"groups of three or more legally autonomous organizations that work together to achieve not only their own goals but also a collective goal."*

Smart business networks are then defined by Van Heck and Vervest (2007) as networks that include additional layers of meaning—from the business operating layer, transaction layer to logistics layer to seek linkages that are crucial to attain sustained competitive advantage. They also argue that the essential features of smart business networks are their capacity to "rapidly pick, plug in and play" business processes to configure to a particular goal quickly and that the link between the business network's strategy and structure and the underlying infrastructure is key to smart business networks. Vervest et al. (2004) further explain that a smart business network *"segregates the business logic from the executional processes and activities; that is, it*

creates a business operating system. This business operating system coordinates the processes among the networked businesses, and its logic is embedded in the systems used by these businesses."

Additionally, an important part of a smart business network is networkability which Alt and Smits (2007) define as *"the capability of a network to collaborate internally and externally at the level of business processes and underlying IT infrastructure."*

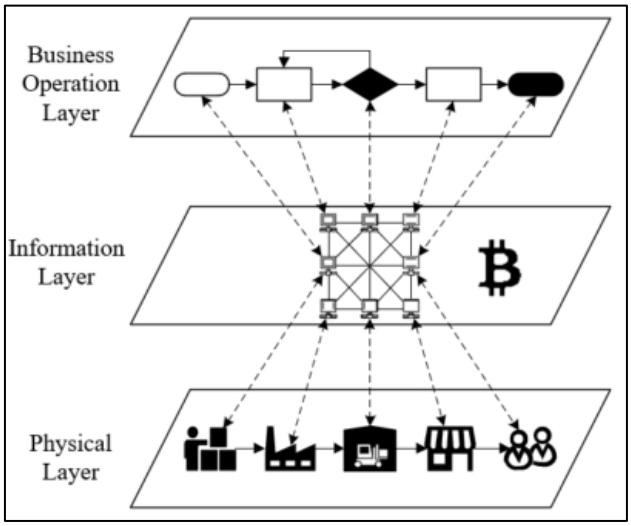
Businesses have inter-organizational relationships in order to improve their own business and performance (Clark & Lee, 2000; Ring & Van de Ven, 1994). Moreover, Barringer and Harrison (2000) explain that there are ten advantages in networks (inter-organizational relationships): "Gain access to a particular resource," "Economies of scale," "Risk and cost-sharing," "Gain access to a foreign market," "Product and/or service development," "Learning," "Speed to market," "Flexibility," "Collective lobbying," and "Neutralizing or blocking competitors" and eight disadvantages: "Loss of proprietary information," "Management complexities," "Financial and organizational risks," "Risk becoming dependent on a partner," "Partial loss of decision autonomy," "Cultures of partners may clash," Loss of organizational flexibility," and "Antitrust implications."

Smits and Hulstijn (2020); Van Heck and Vervest (2007) argue that business networks have three layers:

- Business Operation Layer: the layer that represents the business processes.
- Information Layer: the layer is where data on transactions are stored.
- Physical Layer: the layer that represents the entity's operations involved in the business network.

Figure 5

Three Business Network Layers



Note. Adapted from "Blockchain Applications and Institutional Trust," by M.Smits and J.Hulstijn, 2020, *Frontiers in Blockchain*, *3*(5), p. 4 (https://doi.org/10.3389/fbloc.2020.00005). CC-BY-NC.

2.2.1 **Performance of the Network**

Smits (2002) states that five variables of the network influence the performance of the network are:

Table 2

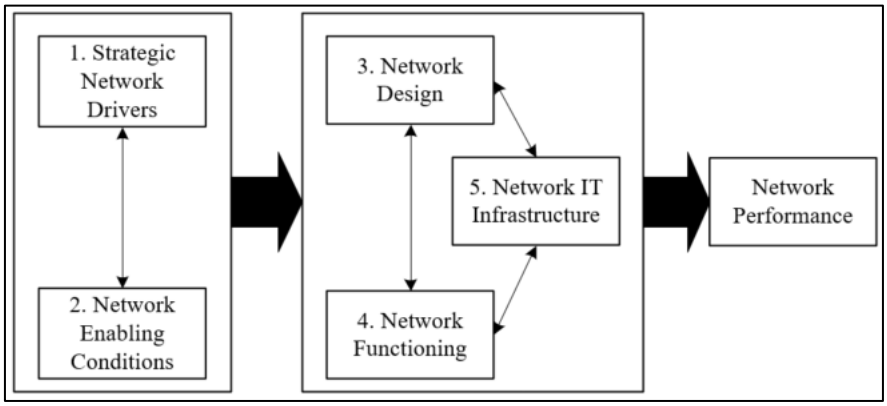
The Five Factors for Determining Network Performance

Strategic Network Drivers	Network Enabling Conditions	Network Design	Network Functioning	Network IT Infrastructure
Organizations and stakeholders participate in the network's aims, motivations, views, and expectations.	The factors that allowed or facilitated the network's creation and development.	Configuration, duties, decision-making divisions, and governance mechanisms of the network.	The network's inter-and intra-organizational operations and procedures.	Self-explanatory

Note. Adapted from "Performance and development of electronic business networks," by M.Smits, 2002, *Innovative Business Models in the Network Economy*, p. 4 (https://research.tilburguniversity.edu/en/publications/performance-and-development-of-electronic-business-networks). Copyright 2002 by Martin Smits.

Figure 6

Conceptual Model of the Five Factors for Determining Network Performance



Note. Adapted from "Performance and development of electronic business networks," by M.Smits, 2002, *Innovative Business Models in the Network Economy*, p. 4 (https://research.tilburguniversity.edu/en/publications/performance-and-development-of-electronic-business-networks). Copyright 2002 by Martin Smits.

Key elements

Consortium blockchains fulfill the elements of a 'smart business network' to be recognized, like having a collective network goal, "rapidly pick, plug in and play" of business processes to configure to a particular goal quickly and that the link between the business network's strategy and structure and the underlying shared IT infrastructure (DLT). Thus, due to smart business network theory, the formation of a consortium blockchain can be understood, and the network's factors for determining the network performance of the consortium blockchain.

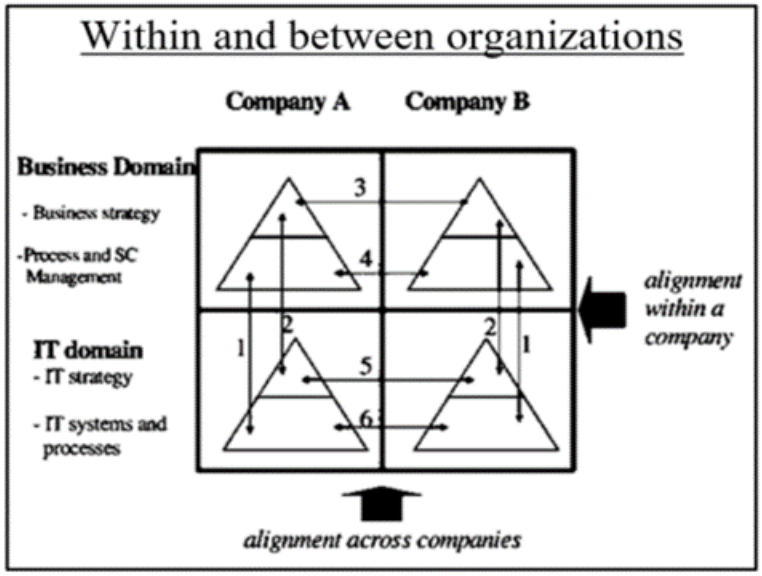
Moreover, Barringer and Harrison (2000) explain the advantages and disadvantages of networks that also can apply to consortium blockchain.

2.3 Extended Strategic Alignment Model

According to Straub et al. (2004), there is little information on the alignment of IT and several businesses in a network that makes IT and business decisions independently. Torabkhani et al. (2007) state that the Strategic Alignment Model (SAM) has focused on one organization, so they researched business-IT alignment within a network to determine to what extent a business network's overall performance is impacted by the degree of (extended) strategic alignment. To analyze the alignment processes between business and IT domains within an organization and across organizations in a business network, Torabkhani et al. (2007) developed the 'extended strategic alignment model.' See figure 7.

Figure 7

Extended Strategic Alignment Model (ESAM)



Note. From "Improving the Performance of Business Networks in E-Government," by R.Torabkhani, M.Smits, and G.van der Pijl, 2007, *Annals of Operations Research*, 20th Bled eConference eMergence), p. 64 (https://www.researchgate.net/publication/254800822_Improving_the_performance_of_business_networks_in_E-government). In the public domain.

It starts with an inventory of the current IT, IOS (Inter-Organizational System), and IT infrastructure of the firms in the network are necessary. This extended alignment involves documentation of the business operations, IT operations, IT strategies, and information flows across and among network participants. Luftman (1996) defines alignment sequence as procedures that consist of the following three components:

- **Driver:** the domain that initiates a process or objective.
- **Lever:** the leveraging mechanism to achieve a significant impact.
- **Impact:** the result of the process that has a positive or negative effect on the other domain.

There are eight alignment sequences consisting of four business side initiatives and four IT side initiatives. Four of these eight are dominant alignment sequences (marked as bold text). See table 3.

Table 3

Eight Alignment Sequences

Business Side Initiative		IT Side Initiative	
Strategy Execution	Driver: Business Strategy Lever: Business Operation Impact: IT Infrastructure	**Competitive Potential**	Driver: IT Strategy Lever: Business Strategy Impact: Business Operation
Technology Potential	Driver: Business Strategy Lever: IT Strategy Impact: IT Infrastructure	**Service Level**	Driver: IT Strategy Lever: IT Infrastructure Impact: Business Operation
Organization IT Infrastructure	Driver: Business Operation Lever: IT Infrastructure Impact: IT Strategy	IT Organization Infrastructure	Driver: IT Infrastructure Lever: Business Operation Impact: Business Strategy
Organization Infrastructure Strategy	Driver: Business Operation Lever: Business Strategy Impact: IT Strategy	IT Infrastructure Strategy	Driver: IT Infrastructure Lever: IT Strategy Impact: Business Strategy

Note. Adapted from *Competing in the Information Age: Strategic Alignment in Practice*, by J.N.Luftman, 1996, P. 45, 64, Oxford University Press Inc (https://books.google.nl/books/about/Competing_in_the_Information_Age.html?id=LxzjXmR2pIEC&printsec=frontcover&source=kp_read_button&hl=en&redir_esc=y#v=onepage&q&f=false). Copyright 1996 by Oxford University Press Inc.

To help align the eight domains accordingly and thus achieve strategic alignment or control, Luftman (1996) identified four alignment control mechanisms:

1. **Value management:** the means that ensures that IT investments get the most gain.

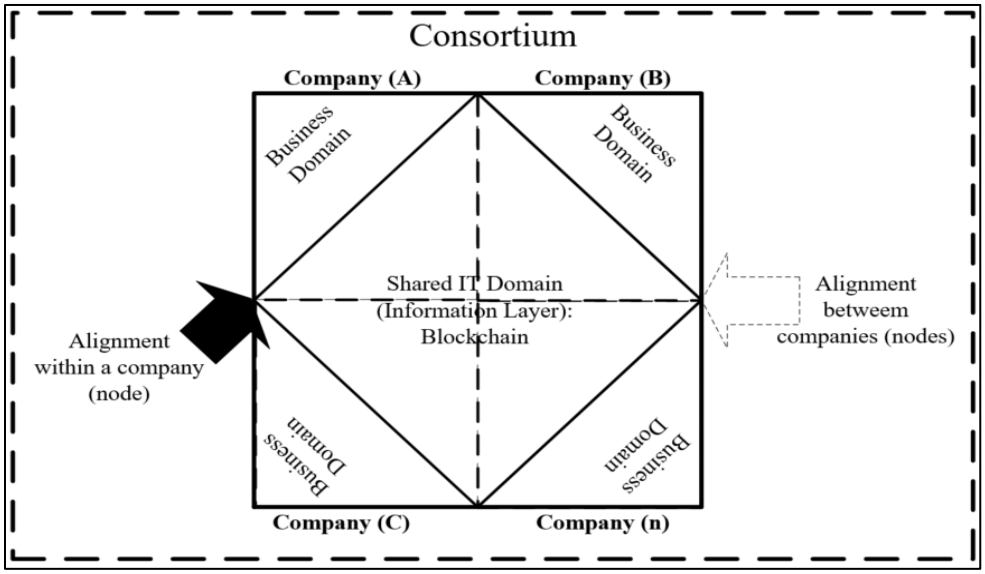
2. **Governance:** the means to establish the distribution of decision-making responsibilities among executives or business partners.
3. **Technological capability:** the means through which the different IT capabilities necessary to support and influence business strategy can be specified and modified.
4. **Organizational capability:** the means that defines, modifies, and even reinvents the many skills and processes needed to support and influence business strategy.

Key Elements

The ESAM provides an overview of how multiple businesses need to align. In the case of the consortium blockchain, the participants share the same on-chain IT infrastructure. Only explicit focus is needed on business alignment, which is business operation and off-chain related. The DLT in the consortium can be considered the IOS (Inter-Organizational System). For that reason, a suitable alignment sequence for consortium blockchain could be the Service Level alignment (driver: IT Strategy, lever: IT Infrastructure, and impact: Business Operation) because of the unique leverage in the consortium, which is a shared IT infrastructure in the form of DLT. Follow-ups, in this case, could be procedures like documentation of the business operations, IT operations, IT strategies, and information flows across and among network participants. Furthermore, this study will discuss the alignment control mechanism: Governance, focusing on Network Governance to achieve strategic alignment in the upcoming chapter.

Figure 8

ESAM of the Consortium Blockchain (based on Torabkhani et al.,2007)



Note. From “Improving the Performance of Business Networks in E-Government,” by R.Torabkhani, M.Smits, and G.van der Pijl, 2007, *Annals of Operations Research*, 20th Bled eConference eMergence), p. 64 (https://www.researchgate.net/publication/254800822_Improving_the_performance_of_business_networks_in_E-government). In the public domain.

2.4 Network Governance

Provan et al. (2007) discuss networks that are frequently systematically constructed and controlled, and purpose-focused rather than emerging serendipitously. The authors further argue that it is important to know what governance mechanism governs the network, ranging from self-governance and hub-firm/lead organization to network administrative organization (NAO).

According to Eisenhardt (1989), to ensure that the day-to-day operations of an entity(es) are properly overseen and controlled, the function of governance in all of these areas is crucial and is in line with the principal-agent theory. Moreover, Provan and Kenis (2008) state that board members are held accountable for the actions of the entity they represent if such actions are unlawful or inappropriate. An important note is that network governance can lead to network effectiveness, which is *"defined here as the attainment of positive network-level outcomes that could not normally be achieved by individual, organizational participants acting independently."*. (Provan & Kenis, 2008).

Freeman and Evan (1990) even argue that stakeholders would be irrational if they gave up the right to vote and the capacity to monitor the firm's real impact on them, and thus it makes sense for stakeholders to join the board of directors to govern. That is why Provan and Kenis (2008) have developed three basic forms of network governance:

- **Shared Governance (Participant-Governed Network):** Network governance forms whereby the network participants govern the network. These networks are highly decentralized until all network members interact relatively equally in the governance process. This form of network needs the participation and commitment of all or a large portion of the network's organizations. Network members manage internal and external connections and activities. Participants will only be dedicated to the network's aims if all members contribute equally.
- **Lead Organization:** in the lead organization form, an administrator manages the networks, all significant network-level activities, and critical decisions. Thus, network

governance is highly centralized. A lead organization administers the network or helps member organizations accomplish network objectives, which may coincide with the lead organization's aims. The lead organization may pay for network management, accept donations from network members, or seek grants or government financing. The members may choose the lead organization based on what appears most efficient and effective, or an external funder may impose it.

- **Network Administrative Organization:** the NAO form. A separate administrative organization governs the network's operations. The NAO form is centralized, yet network members still interact. The network broker (NAO) coordinates and maintains the network. Unlike the lead organization model, NAO is not a member organization delivering its own services. The network is externally managed by the NAO, which the members create. The NAO may be a government agency or a nonprofit, even when network members are for-profit firms. The NAO may be a government agency or a nonprofit, even when network members are for-profit firms.

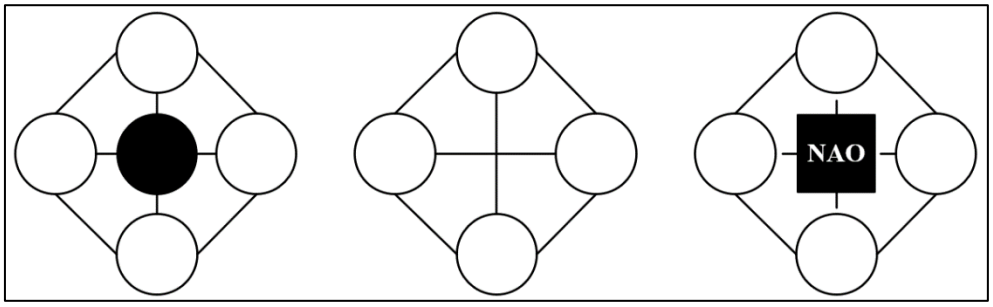
Similarly, Hulstijn et al. (2016); Steinfield et al. (2011) explain that there are different forms of network configurations, namely:

- **Hierarchical:** there is a clear representation for the assertive partner, who will also be in a position to transfer risks and controls;
- **Peer-to-Peer (P2P):** in the absence of a prominent partner, the chosen representative functions as the official representative, and;
- **Membership:** in this type of configuration, participation in a cooperative implies influence.

Figure 9 summarizes both ways of configurations.

Figure 9

Network forms: (a) Lead Governance/Hierarchical, (b) Shared Governance/P2P, (c) NAO/Membership



Note. Adapted from "Towards Trusted Trade-Lanes," by J.Hulstijn, W.Hofman, G.Zomer, and Y.Tan, 2016, *Electronic Government*, *9820* (1), p. 306 (https://doi.org/10.1007/978-3-319-44421-5_24). Copyright 2016 by IFIP International Federation for Information Processing.
And Adapted from "Modes of network governance," by K.G.Provan and P.N.Kenis, 2008, *Journal of Public Administration Research and Theory*, *18* (2), p. 6-8 (https://doi.org/10.1093/jopart/mum015). In the public domain.

Key elements

Network governance is an important part of a smart business network in the design and administration of the network. Provan and Kenis (2008) sum up the key predictors of the effectiveness of network governance forms. See table 1. It is important to distinguish the types of consortium blockchains and explain their characteristics in terms of trust. Until now, consortium blockchains have been divided into business-focused, technology-focused, and dual-focused. It is interesting to see how the above distinction aligns with Provan and Kenis (2008) their categorization.

Table 4

Key Predictors of Effectiveness of Network Governance Forms

Governance Forms	Trust	Number of Participants	Goal Consensus	Need for Network Level Competencies
Lead Organization/ Hierarchical	Low density, High centralization	Decent amount	Decently Low	Decent
Shared Governance/P2P	High density, High decentralization	Few	High	Low
NAO/Membership	Moderate density, NAO monitored by members	Decent to Many	Decently High	High

Note. Adapted from "Modes of Network Governance: Structure, Management, and Effectiveness," by K.G.Provan and P.Kenis, 2007, *Journal of Public Administration Research and Theory*, *18*(2), p. 9 (https://doi.org/10.1093/jopart/mum015). Copyright 2007 by The Author.

2.5 Model of Trust

The Model of Trust developed by Mayer et al. (1995) describes inter-organizational trust. Mayer et al. (1995) define trust as *"the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party."* Mayer et al. (1995) conclude that trust is founded on ability, benevolence, and integrity, also known as the Factors of Perceived Trustworthiness and the trustor's propensity described below.

Ability refers to the collection of abilities, competencies, and traits that allow a party to exert influence within a specific area (Mayer et al., 1995).

Benevolence refers to the degree to which a trustee is regarded to want to do good for the trustor, in addition to egotistical profit motivation. Benevolence is the impression of a trustee's favorable attitude toward the trustor (Mayer et al., 1995).

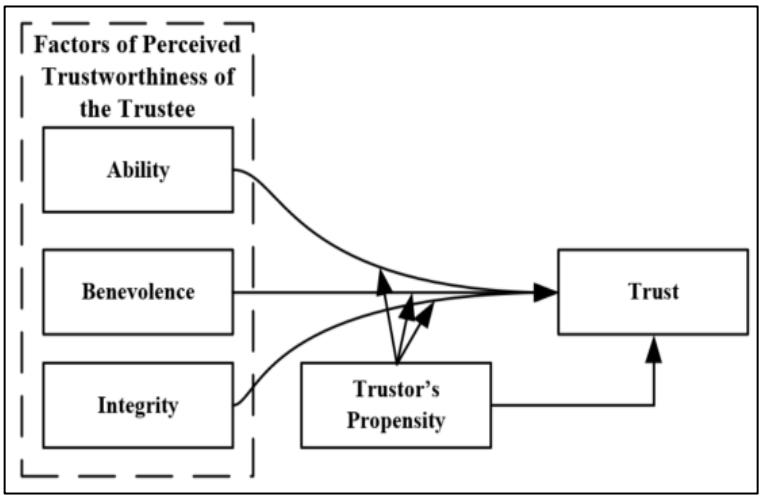
Integrity refers to the trustor's impression of the trustee adhering to a set of standards deemed acceptable by the trustor (Mayer et al., 1995).

Trustor's propensity can be described as the tendency of the trustor either to take or avoid risks (Mayer et al., 1995).

The above variables result in the following model adapted model of Mayer. See figure 10.

Figure 10

Model of Trust



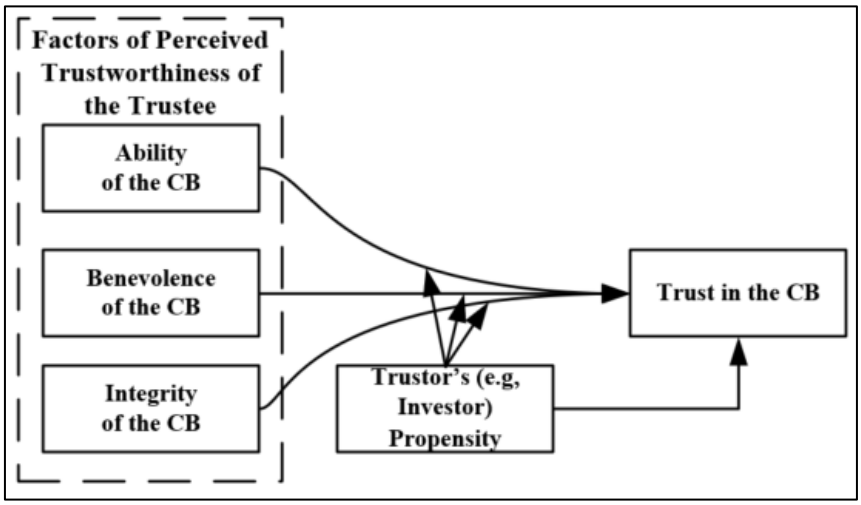
Note. Adapted from from "An Integrative Model of Organizational Trust," by R.C.Mayer, J.H.Davis, and F.D.Schoorman, 1995, *The Academy of Management Review*, *20*(3), p. 715 (https://doi.org/10.2307/258792). Copyright 1995 by Academy of Management.

Key elements

The theory of Mayer gives this study the requirements (ability, benevolence, integrity) for trust in the inter-organizational relationship: the consortium. Trust refers to this model as the trust between the investor or shareholder and the consortium blockchain. As seen in the revised model in figure 11, trust is based on the factors of trustworthiness (ability, benevolence, and integrity) of the consortium blockchain and the trustor's (e.g., investor or shareholder) propensity to trust the consortium blockchain in which it wants to invest in for example.

Figure 11

Revised Model of Trust (based on Mayer, 1995)



Note. Adapted from from "An Integrative Model of Organizational Trust," by R.C.Mayer, J.H.Davis, and F.D.Schoorman, 1995, *The Academy of Management Review*, *20*(3), p. 715 (https://doi.org/10.2307/258792). Copyright 1995 by Academy of Management.

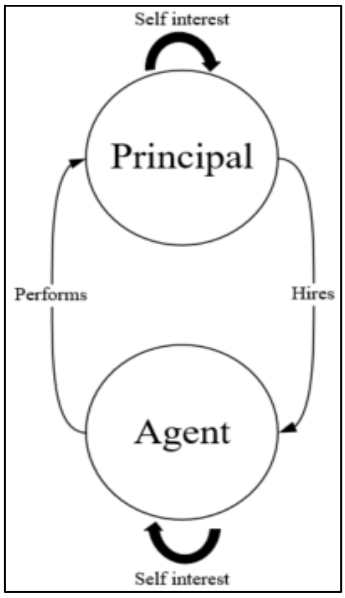
2.6 Agency Theory

The agency theory is one of the most well-established and often defined ways of communication and is concerned with the issues that arise when a principal delegates responsibilities to an agent in the setting of competing interests; this by beginning their business relationship by agreeing on a payment, which is based on some percentage of the outcome of the agent's work (Linder & Foss, 2013; Ross, 1973). Fields like accounting, economics, finance, marketing, politics, organizational behavior, and sociology have all used the agency theory (Eisenhardt, 1989). Ross (1973) states that the agent-principal relationship has been established when one party acts on behalf of or behalf of the other in a specific sphere of decision-making issues. The principal (e.g., shareholder, customer, client, etc.) is the one that delegates a physical

or mental work to the agent (e.g., director, staff, seller, specialist, etc.) whose choices of actions or effort level affect the rewards for both parties (Jensen & Meckling, 1976). Linder and Foss (2013) state that reasons for delegating task(s) may be due to lack of time (efficiency) or knowledge and expertise of the task (effectively), and because of this, the principal has a hard time determining the agent's true level of knowledge or effort. See figure 12 for visual representation.

Figure 12

Principal-Agent Relationship



Note. Adapted from "Agency Theory: An Assessment and Review," by K.M.Eisenhardt , 1989, *The Academy of Management Review*, *14*(1), p. 59-62 (https://doi.org/10.5465/amr.1989.4279003). Copyright 1989 by Academy of Management Review.

Eisenhardt (1989) mentions that the agency theory covers two issues that might arise in agency interactions. One difficulty emerges when there is a conflict of interest, and the second is the impossibility for a principal to verify what the agent really is doing. As a result, the principal and the agent may choose different behaviors based on their risk preferences. Eisenhardt (1989) also states that the most effective contract structure for controlling the principal-agent engagement should represent efficient information and risk-bearing cost arrangement in principal-agent partnerships. Linder and Foss (2013) state that agency theory is concerned with two major problems, ex-ante (hidden characteristics) and ex-post (moral hazard/hidden action). The problem of ex-ante 'hidden characteristics' derives from the fact that asymmetry exists before the principal hires an agent; when to get the contract, the agent hides their true skills and even fakes their credentials to get the contract. Linder and Foss (2013) further mention that this

problem is considered one of the most difficult issues in delegation when there are competing interests and an information gap between the participants.

Ex-post (hidden action), on the other hand, is the principal's lack of insight into what the agent really is doing and if the results are due to the agent's effort or just luck; hence, both information asymmetry and conflict of interest are necessary ingredients for a 'principal-agent problem' to exist. (Linder & Foss, 2013).

2.6.1 Agency Theory in Audit

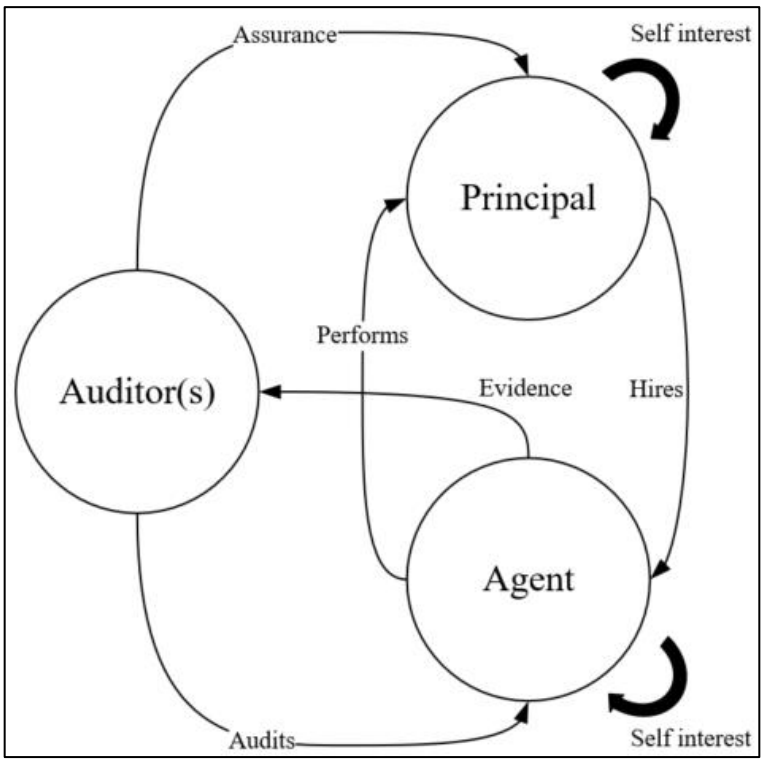
The Audit and Assurance faculty magazine Audit Quality (2005) states that agency theory is a valuable economic theory of accountability that may be used to explain the evolution of auditing. Colbert and Jahera Jr (1988) state that there are several ways the agency theory may be used to explain the link between internal audit and external audit and the relationship of the auditors with the management, board of directors, and shareholder interactions. According to the fundamentals of economics, people are motivated by the desire to maximize their personal utility (Colbert & Jahera Jr, 1988). That is where various mechanisms may be employed to attempt to match the interests of agents with principals and enable principals to assess and regulate the behavior of their agents and encourage confidence in agents (Audit Quality, 2005). One of these mechanisms is the audit function that exists to oversee management's (agent) actions and certify management's (agent) achievement for the benefit of the board of directors (principal) or shareholders (principal). However, managers and inside shareholders may also be reassured by the audit function that this objective is not being violated to harm other shareholders (Colbert & Jahera Jr, 1988).

Key elements

The agency theory explains the principal-agent relationship, the problems, and possible mechanisms to solve these problems. Eisenhardt (1989) states that "*when the principal has information to verify agent behavior, the agent is more likely to behave in the interests of the principal.".* A key mechanism to align interests is to involve a third-party auditor, thus giving importance to audit & assurance as a solution for the principle-agent relationship. Audits assist in retaining trust and confidence through an impartial check on the work of agents and evidence given by the agents. To continue to assure the investor or shareholder (principal) and audit consortium blockchain, standards are needed.

Figure 13

The Auditor as Mechanism in the Principal-Agent Relationship



Note. Adapted from "Auditing" by J.Hulstijn, 2020, *Cybersecurity Risk Management course, Tilburg School of Economics and Management*, Slide 3. Copyright 2020 by Joris Hulstijn. Reprinted with permission.

2.7 Audit & Assurance

This chapter is compact because the study is directed to IT auditors. Nonetheless, a short explanation will be given about assurance & audit, procedures, the auditor's role, and types of norms for non-audit readers.

2.7.1 Assurance

Assurance services are independent professional services that enhance the quality or context of information for decision-makers and are issued by Certified Public Accountants (CPAs). The CPA can review any financial document or transaction, such as a loan or contract to confirm the accuracy and validity of the subject under examination (Deloitte, n.d.-b). The reason for assurance is *"to provide a service that increases confidence in the information, the independent professional providing it has to engender trust, not only as a provider of the service but also in the process the professional uses to deliver it."*. (AICPA, 2013).

2.7.2 **Audit**

Silvoso (1972) defines audit as "*a systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between those assertions and established criteria and communicating the results to interested users."*. There are different kinds of audits like a financial audit, operational audit, compliance audit, and of course, IT audit. An Information Technology audit reviews a company's information technology systems to determine whether or not such systems are being managed in line with the company's overall goals and objectives (Deloitte, n.d.-a). Classification is also done as an internal audit and external audit.

2.7.3 **IT Audit Procedures**

The IT audit procedures are comparable to the basic audit procedures as described by the U-C Section 33: Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained. Central to the procedure is the test of controls which is the procedure to assess the efficacy of controls in preventing, detecting, and correcting, substantial misstatements in an assertion level audit. This testing is done through evaluating samples via sampling methods like inquiry, observation, reperformance, and inspection.

2.7.4 **The Role & Responsibility of the Auditor**

The auditor follows the auditing standards and requirements of the local countries and performs their audits in accordance with fundamental ethical principles and with an attitude of professional skepticism. There are three general principles an auditor has to comply with:

- Like law and medicine, the accounting profession has a code of ethics, which the auditor should comply with at all times unless laws and regulations in specific circumstances preclude certain parts.
- The auditor should comply with the Code of Ethics for Professional Accountants issued by the International Federation of Accountants (IFAC). IFAC believes that the identity of the accountancy profession is characterized worldwide by its endeavor to achieve several common objectives and by its observance of certain fundamental principles for that purpose.
- IFAC, recognizing the responsibilities of the accountancy profession and considering its own role to be that of providing guidance, encouraging continuity of efforts, and promoting harmonization, has deemed it essential to establish the International Code

of Ethics for Professional Accountants to be the basis on which the ethical requirements for professional accountants in each country should be founded (EY).

2.7.5 Principle-based vs Rule-based norms

Two forms of norms are the basis for legislation and regulation systems: rule-based and principle-based (Schilder, 2008). Rule-based norms lay out the rules of conduct and what exactly should be done, whereas principle-based formulates norms as guides, leaving the specific application to the user of the norm (Burgemeestre et al., 2009). In rule-based, there is confidence in knowing that when the audited entity follows the rules, it will comply. However, this means that a rule-based system needs more work from the regulator since the specifics need to be specified in advance. Whereas in principle-based, the effort is from the subject side. Table 5 shows per dimension the difference between principle-based and rule-based norms.

Table 5

Characterization of rules and principles by dimensions

Dimension	Principles-based	Rules-based
Temporal	Ex post	Ex ante
Conceptual	General/universal/abstract	Specific/particular/concrete
Functional	Large voluntary power	Little voluntary power
Representation	Declarative (what)	Procedural (how)
Knowledge needed	Quite a lot	Relatively little
Exception handling	Allow for exceptions (defeasible)	All or nothing (strict)
Conflict resolution	By weight (trade off)	No conflicts possible

Note. Adapted from "Rule-based versus Principle-based Regulatory Compliance," by B.Gurgemeestre, J.Hulstijn, and Y.Tan, 2009, *Frontiers in Artificial Intelligence and Applications*, p. 39 (https://ebooks.iospress.nl/publication/5520). Copyright 2021 by IOS Press.

Key Elements:

Burgemeestre et al. (2009) conclude that when it comes to the adoption and auditing tasks, the observed variations may be explained by the necessity to pick and weigh applicable principle-based on context-relevant data. This weighting is a task where specialized knowledge is needed, and IT generally needs very exact and thorough specifications. Therefore, principle-based norms will be used instead of rule-based norms, as this thesis study develops a conceptual audit framework for consortium blockchain. In that case, Burgemeestre et al. (2009) further explain that principles must first be adjusted to the unique context of an organization before principle-based norms can be applied. Principle-based regulation is often accomplished by first identifying control goals and then designing a system of control measures that can be

implemented as system rules. Which indeed provides the flexibility that further requires the auditor's professional judgment.

3 Theoretical Framework

Several theories and topics were discussed in the literature review related to the research questions. These topics can be categorized into three groups: (1) Consortium Blockchain, (2) Network, Alignment & Governance, and (3) Trust, Agency, Audit & Assurance. Based on all discussed theories, a summarizing and holistic model is developed to understand auditing consortium blockchains, see figure 14.

3.1 ABC Model

The ABC (Auditability Blockchain Consortium) Model is developed based on previously discussed models and theories. The ABC model summarizes the core components of the theories Smart Business Network, ESAM, Network Governance, Model of Trust, and Agency theory to have a clear overview of the relationship between the external auditor, the consortium blockchain client, and the investor. The model consists of different parts discussed below:

Principal/trustor/auditor's client

The principal/trustor in this model is the investor or shareholder who wants assurance to trust the consortium blockchain or not. An important part is the tendency of the investor to either take or avoid the risk of trusting the consortium, which is the investor's propensity.

Agent/Trustee/Consortium

The agent/trustee in this model is the consortium blockchain, which consists of a collaboration of participants with a common goal using a private DLT.

NAO

The NAO (Network Administrative Organization) is a separate administrative organization that governs the network consisting of network members who are voted to join this board organization. Thus, the NAO is not a member organization of the network delivering its own services but is only responsible for coordinating the network.

Businesses Alignment

Because of the shared IT infrastructure/information layer between consortium members, it is necessary that the business domain of the participants also need to align to achieve a common goal and to prevent conflict of interest between participants.

Auditor

The auditor in the model is an external auditor (firm) who audits the NAO with the Consortium Blockchain Audit Control Framework, taking factors of perceived trustworthiness into account. These adapted factors are:

Ability: the collection of the consortium blockchain's abilities, competencies, and traits that allow the network to exert influence within a specific area.

Benevolence: the degree to which a consortium blockchain is regarded to want to do good for the investor in addition to egotistical profit motivation.

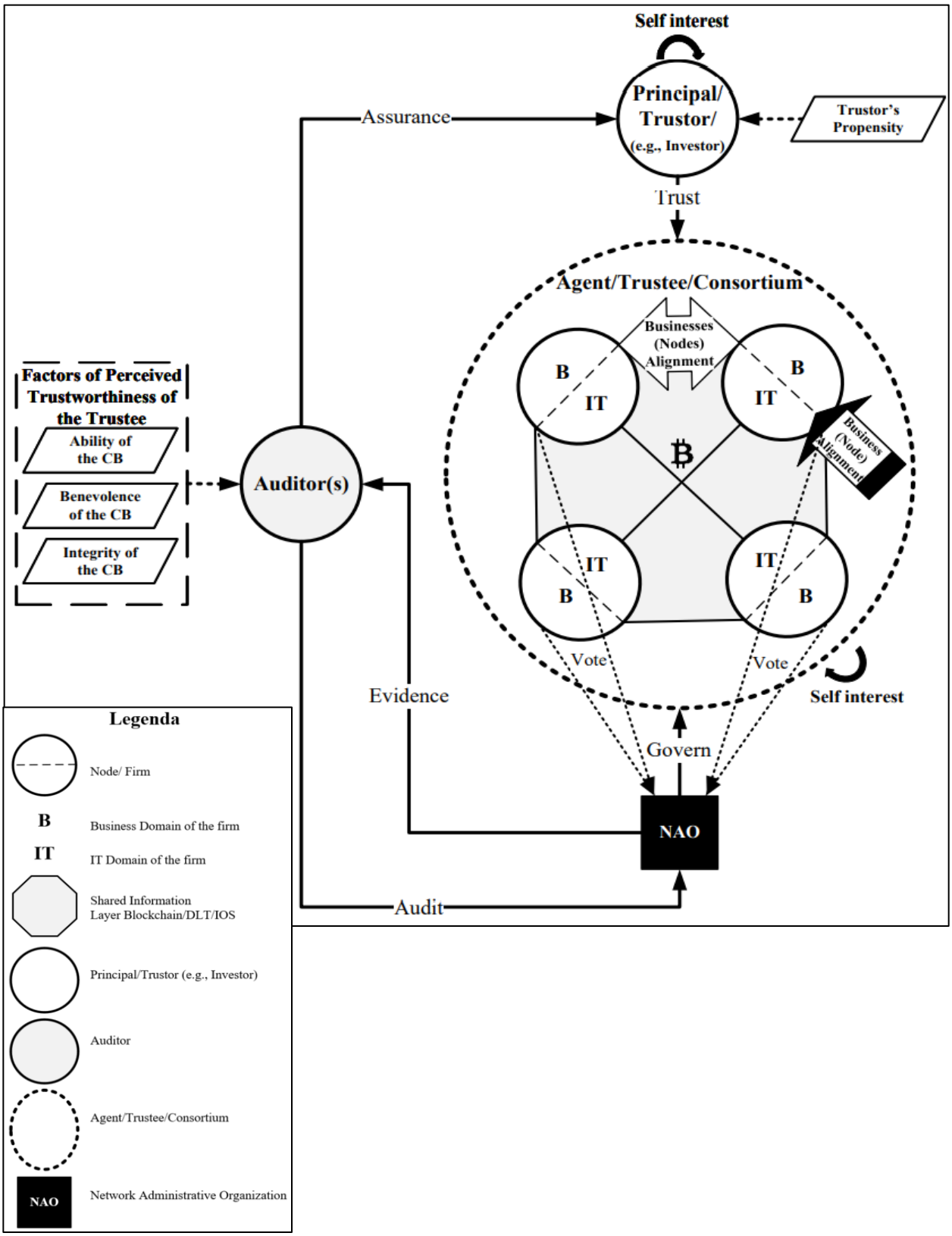
Integrity: the degree to which the consortium blockchain adheres to a set of standards deemed acceptable by the investor or shareholder.

Process

The starting point of this model is the principal-agent/trustor-trustee relationship. To assure the investor or shareholder (principal/trustor), a key mechanism in the form of a third-party auditor is involved in auditing the consortium (agent/trustee) since it is more probable that the consortium will act in the investor's best interests if the investor receives information verifying the consortium their actions (Eisenhardt, 1989). Audits assist in retaining trust and confidence through an impartial check on the NAO's work composed of the consortium members chosen to represent the consortium. The auditor in the model is an external auditor (firm) who is not part of the consortium like the NAO. The auditor audits the NAO, who represents the consortium members and is responsible for delivering evidence for audit work. Part of the audit work is to check for alignment between the organizations in the consortium in how well their business domain align with each other. The other part is to see if the business & IT within one organization is aligned. After that, the auditor can assure the investor or shareholder who can trust the consortium. Trust is in this model adapted from Mayer et al. (1995) and means the readiness of the principal/trustor/investor to be exposed to the agent/trustee/consortium's actions because the investor expects the consortium to accomplish a certain activity that is significant to the investor.

Figure 14

ABC (Auditability Blockchain Consortium) Model



4 Methodology

This chapter discusses the research -approach, -method, -paradigm, -framework, -design (-type and -strategy), and -process.

4.1 Research Approach

This thesis has an inductive approach due to the absence of prior theory on the auditability of consortium blockchain. Therefore it follows the inductive procedures of defining the business problem followed by formulating the problem statement, providing a conceptual background, choosing a research design (research type, research strategy, and sampling design), and collecting data. After data collection, the study analyzes the data to develop an artifact, that is, the development of a concept standard for auditing consortium blockchain(s). Even though the research is held within EY, the results may not be exclusive to EY due to the artifact's general nature derived from different international standards. Hence, the study has a fundamental nature as opposed to applied research, which is single firm-specific.

4.2 Research Method

Locke et al. (2013) argue that the researcher should answer the question of why they should do qualitative research. In this case, this research is exploring the auditability of a blockchain due to the lack of research on it and the missing standard(s) for auditing blockchain. To achieve this, interviews are held with blockchain experts and IT auditors at EY, NEN, and three different consortium blockchains. Moreover, internal desk research is conducted where relevant information is collected within EY, and external desk research collects information from open databases and sites.

4.3 Research Paradigm

Hevner et al. (2004) argue that two paradigms are the foundation of the IS discipline: behavioral science and design science. The behavioral science paradigm aims to create and test theories that may be used to predict or explain human or organizational behavior. The design-science paradigm aims to push the frontiers of human and organizational capabilities by generating new and inventive objects. This research is inductive due to a business need for an audit standard(s) for (consortium)blockchain, resulting in an artifact. For this reason, the design science paradigm is deemed appropriate; therefore, this study conducts design science research.

Design science is constructing and exploring artifacts in context (Wieringa, 2014). According to Wieringa (2014), Design science is about solving three types of problems:

- Knowledge Problem: condition of knowledge does not align with the observer.
- World Problem: the world (or organization) does not align with the observer.
- Design Problem: when the artifact does not exist or does not align with the observer.

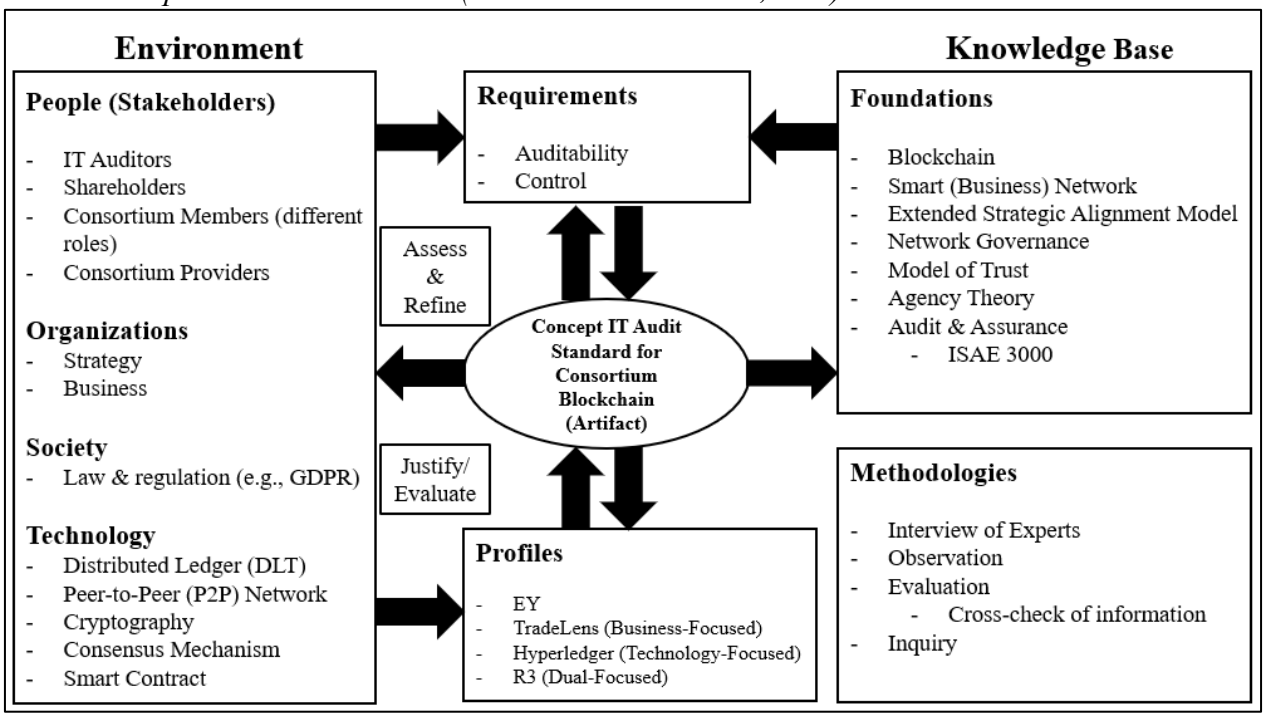
This study focuses on the design problem as there is currently no audit standard for consortium blockchain. Moreover, a design problem is often motivated by a world problem, which is the assurance of consortium blockchain.

4.4 Research Framework

This research assimilates the research framework provided by Hevner et al. (2004) for understanding information systems research and criteria for performing and assessing effective design-science research. Because of using the design science research paradigm, a problem domain and its solution are learned and understood via the construction and use of the designed artifact. Artifacts made to suit a specific business requirement are the focus of DSR, and they aim to be useful. See figure 15.

Figure 15

Filled in template DSR Framework (based on Hevner et al.,2004)



Note. Adapted from "Design Science in Information Systems Research," by A.R.Hevner, S.T.March, J.Park, and S.Ram, 2004, *MIS Quarterly*, *28*(1), p. 80 (https://doi.org/10.2307/25148625). Copyright 2004 by MIS Quarterly.

4.5 Research Design

4.5.1 Research Type

Gregor (2006) distinguishes five types of research:

- **Analysis:** describes what something is and is limited to only analysis and description of the object.
- **Explanation:** describes what, how, why, when, and where something is and explains without the goal of predicting accurately.
- **Prediction:** describes what something is, what something will be, and provides predictions.
- **Explanation and prediction:** describes what, how, why, when, where something is, what something will be, and provides predictions.
- **Design and action:** describe how to do something and gives explicit prescriptions (e.g., methods, techniques, principles) for constructing an artifact.

This study follows a 'design and action' type of research due to the development of an artifact, namely an audit standard of consortium blockchain.

4.5.2 Research Strategy

This study selects the following research strategies based on the chosen research type, design, and action:

Interview: this study tries to increase the interview validity by recording the interviews via Teams or Zoom and transcribing after. As for the reliability, this study uses MS Excel and ATLAS.ti to code and thus compare the output of the interviews finalized in a table. See Appendix D. Also, according to Creswell and Creswell (2017), the total number of questions should be between 5 to 10. In this case, six qualitative open questions are formulated and derived from the research questions.

- **Inquiry:** seeking information from knowledgeable people in (consortium)blockchain, IT audit, and standards throughout or outside of EY.

- **Observation**: Watching processes or procedures being performed by IT auditors within EY and consortium blockchain members of providers B3i, R3, and Hyperledger Foundation.
- **Examination/Inspection:** Examining documents in regards to IT audit or blockchain governance.

Sampling Design

Due to the qualitative nature of this research, this study uses non-probability sampling because non-probability sampling is frequently related to qualitative research (Taherdoost, 2016) To do this research, a proper sampling method is necessary. This method of sampling consists of four types:

- *Quota sampling:* sampling technique where participants are chosen based on specified qualities in order for the overall sample to have the same characteristics distribution as the general population (DAVIS & Cosenza, 2005).
- *Snowball sampling:* sampling technique where a few examples are chosen to motivate others to participate in the study, hence raising the sample size. This strategy works well in tiny groups that are difficult to reach because of their closed character (Brewton & Millward, 2001).
- *Judgment sampling:* sampling technique where in which, in a knowledgeable setting, a person is selected purposefully to provide crucial information that cannot be obtained from people who do not have the specific knowledge
  (Maxwell, 2012).
- *Convenience sampling:* sampling technique, as the name suggests, in which participants are chosen because they are easily accessible, for example, family and friends.

Due to the explorative nature of this research, judgment sampling is considered appropriate where experts in IT audit, standards (NEN), and (consortium)blockchain are purposefully chosen to collect crucial information that cannot be gathered through other means.

Interview protocol

Main question: How should an IT auditor perform an IT audit on a consortium blockchain(s)?

Prior to the interview

Make a video conference (via Teams or Zoom) or a face-to-face interview appointment. In order to save time during the interview, the interviewer sends the interviewee the agenda for the meeting via mail. Make sure the interviewee understands that the results will be kept confidential and not released.

During the interview

Welcome the participant and introduce the participant by name and function. Inquire whether they are willing to be (audio-)recorded so that the interview may be transcribed. Note that due to organizational security measures, Teams recordings are disabled (within EY). Therefore, recording tools like Snagit can be used. The audio tape will only be used to transcribe the interview and will be deleted after the transcribing is done. Also, inquire if the interviewee wants to be mentioned by name and function, just one of the two, or not mentioned at all. Allow interviewees to introduce themselves and provide a description of the research and its purpose. Afterward, start the interview by following the questionnaire. The goal is to collect information on the current governance structure and IT audits.

Post interview

Succeeding the interview, the transcript should be written down word for word, whereby every sentence should be completely typed out. Verify the interviewee's information input. It is also possible to share the transcript with the interviewee before it is processed. Give the interviewee several days to do this task. The transcript should be considered acceptable if there is no response. An analysis of the in-depth interview will then be conducted. In addition, the interviewee can obtain a copy of the interview for consolation. Finally, please provide contact information for eventual questions by the interviewee and thank the interviewee for their time.

Interview Format Consortium Blockchain

1. Could you give a brief history of your consortium and its motives for developing it?
2. What is your [name of the consortium] network?
3. What are the requirements to join the network?
4. Is there a governance body in the network? If so, how is this constructed?

5. What type of consensus mechanism is the network using (e.g., PoW, PoS, etc.)?
6. How do you audit the network? Is there a specific audit entity responsible for this, for example?

Coding

This research uses coding to analyze the interviews. In the coding process, each sentence of the respondent's answer will be assigned a word or short phrase that symbolically assigns a summary variable to analyze and find particular relationships between different interviews. This research follows a combination of grounded theory (inductive coding = developing codes from within the data) and framework analysis (deductive coding = categorizing words, sentences, or paragraphs into predefined codes). The process starts with open coding, where one or more codes are linked to one or more sentences. Next, with axial coding, axial coding the codes are connected logically. Finally, with selective coding, a single, overarching category is chosen that ties together all of the codes and encapsulates the core of the research. The software tool ATLAS.ti is used for a more efficient coding process. For the results, see appendix D.

4.6 Research Process

This study follows the steps of the design science research methodology (DSRM) by Peffers et al. (2007). The DSRM incorporates principles, practices, and procedures required to carry this research and consist out of six steps: problem identification and motivation, the definition of the objectives for a solution, design and development, demonstration, evaluation, and communication. For this research, five out of the six steps are used: problem identification and motivation, the definition of the objectives for a solution, design and development, evaluation, and communication. Step 'demonstration' is taken out due to the availability reasons of the experts.

4.6.1 Research Setting

This research takes place at EY (Ernst & Young) in Rotterdam, the Netherlands, between the 1st of March and the 16th of July 2022. The research will be conducted in the Technology Risk department, part of the Assurance service line of EY (the other three main service lines are: Tax, Consulting, and Strategy & Transactions). This research is specifically carried out in the sub-department of the Technology Risk, SOCR (Service Organization Control Reporting) team, supervised by the company supervisor Ashish Gupta and academic supervisor Joris van Hulstijn.'

4.6.2 Working Method

As mentioned earlier, this research carries out using steps of the DSRM processes.

Problem identification and motivation

It is important to note that this study is iterative, and each step needs a possible revision. This study is inductive due to the absence or little information of prior theory on the knowledge gap, that is, the auditability of consortium blockchain.

First of all, preliminary research is done through desk research which led to the conclusion that EY and other big four companies like Deloitte, PwC, and KPMG are expanding their assurance business by looking at blockchain auditing. Next, the problem indication and statement are developed by looking at three main topics: network, audit & assurance, and blockchain, and crossing them to find the knowledge gap, which is consortium blockchain auditing.

Define the objectives for a solution/ Requirements

Then, in accordance with the company supervisor, the research goal is set by using Wieringa (2014) template: Improve [a problem context] by [(re)designing an artifact] that satisfies [some requirements] in order to [help stakeholders achieve some goals]. Then, the research is scoped down to ISAE 3000 standard as the basis of the artifact, exclusively the SOCR Team part of Technology Risk part of Assurance service line of EY, and consortium blockchain. Then, the research questions are developed and made in alignment with the problem and goal.

Afterward, the literature review provides a conceptual background explaining different standards and theories. The literature study will be primarily using “top journals” and “very good journals,” as mentioned by the thesis regulation board of the master Information Management, papers, inquiries by experts from the blockchain, consortium blockchain providers, and IT auditors; and audit standard ISAE 3000. Additionally, primary sources up to five years old are used to ensure the relevance and quality of the topic. Also, various combinations of the terms’ blockchain,’ ‘Audit,’ ‘Assurance,’ ‘Governance,’ and ‘Trust’ were utilized in search engines like WorldCat, ScienceDirect, and Google Scholar. For this phase, six discussions are held. Three of them are semi-construct interviews, two open interviews, and one workshop. On the grounds of the knowledge gap, the interviewees are categorized into five categories: Standards, IT Audit, Blockchain, Consortium Blockchain, and Audit framework (artifact). The author chooses the participants based on their expertise in the different categories mentioned above. See table 6.

Table 6

Interviews + workshop DSR Phase: Requirements

#	DSR Phase	Type	Topic	Function	Company
1	Requirements	Open interview	Standards	Consultant ICT Standardization	NEN
2	Requirements	Open interview	Blockchain + IT audit	IT Auditor Technology Risk (specialized in Blockchain)	EY Netherlands
3	Requirements	Semi-structured interview	Consortium Blockchain (Dual-focused)	Account Executive	R3
4	Requirements	Semi-structured interview	Consortium Blockchain (Technology-focused)	Ecosystem Manager	Hyperledger Foundation
5	Requirements	Semi-structured interview	Consortium Blockchain (Business-focused)	Head of Market Insights & Development	B3i
*	Requirements	*Workshop*	IT audit	Senior IT Auditor Technology Risk	EY

Design and development

The output of the literature review and interviews were reviewed to develop the artifact and conclusively answer the research question(s). The design starts with the creation of the backbone of the framework. That is the 'topic' section based on academic theories around the network. Each topic consists of three control types: preventive, detective, and corrective. The artifact's purpose is to give the IT auditor a set of principle-based controls to hold and use further professional judgment to review those controls. For developing the artifact, the study follows the seven guidelines given by Hevner et al. (2004):

1. For DSR to be successful, it must create a working construct, a working model, a workable procedure, or a workable instance.
2. DSR's goal is to design technological solutions that address business issues.
3. Establishing a design artifact's usefulness, quality, and effectiveness must be evaluated systematically.
4. For effective DSR, professionals must demonstrate their contributions to the design artifact, design principles, and methodology.
5. DSR depends on the application of proper procedures for both design and assessment.

6. To find a useful artifact, one must use accessible resources while still adhering to the norms of the issue set.
7. Both technical and mangers users should be able to understand DSR.

Furthermore, other frameworks (like by ISACA) were analyzed for input for the CBAC Framework. Moreover, NOREA Congress was attended to gain more understanding of the way of working of the IT auditor. See Appendix E.

Table 7

Interviews DSR Phase: Development

#	DSR Phase	Type	Topic	Function	Company
6	Development	Open interview for cross-check	Audit Control Framework for CB	Consultant (specialized in blockchain)	EY Switzerland
7	Development	Open interview for cross-check	Audit Control Framework for CB	Assistant Manager (specialized in blockchain)	EY Switzerland
8	Development	Open interview for cross-check	Audit Control Framework for CB	Senior Consultant Technology Risk (specialized in blockchain)	EY Belgium

Evaluation

For the evaluation phase, four open interviews were held. See table 8. During the interview, the interviewer keeps track of the artifact and evaluates how well it supports the solution to the issue. Whether iteration is needed is depended on how preciously the results align with the initial requirements. It is also important to cross-check the information in order to validate its reliability of the information by having multiple interviews on the same topic.

Communication

Explain the issue and the artifact's significance to practicing professionals, in this case, the IT auditors. This study is done by having a final conversation with the EY blockchain expert and handing over the Consortium Blockchain Audit Control Framework.

Table 8

Interviews DSR Phase: Evaluation

#	DSR Phase	Type	Topic	Function	Company
9	Evaluation	Open interview for cross-check	Evaluating Audit Control Framework	IT Auditor Technology Risk	EY Netherlands
10	Evaluation	Open interview for cross-check	Evaluating Audit Control Framework	IT Auditor Technology Risk	EY Netherlands
11	Evaluation	Open interview for cross-check	Evaluating Audit Control Framework	Senior Manager Technology Risk	EY Netherlands
12	Evaluation & Communication	Open interview for cross-check	Evaluating Audit Control Framework	IT Auditor Technology Risk (specialized in Blockchain)	EY Netherlands

5 CB Findings

In this chapter, a compilation of the most significant findings based on the interviews with three consortium blockchain providers (respondents 3 (R3), 4 (Hyperledger Foundation), and 5 (B3i)) are discussed.

5.1 Off-chain Focused

A crucial finding is about the focus on off-chain governance. This finding also corresponds with findings derived from the interviews with consortium blockchain providers is, that the focus of standards should be on off-chain. R3 states: *"On-chain governance like DAOs (decentralized autonomous organizations) are new and have many risks involved, such as mistakes in smart contracts. For this matter, most consortium blockchains should also take an off-chain approach that is more traditional governance by organizations. Criteria for choosing the right entity could be the geographical area of the founding members or area jurisdiction. For example, if a consortium of European businesses decides to form a governing body, it is logically and likely to settle in Europe instead of Asia. Another factor of successful governance is that all stakeholders should be recognized, and decision-making power should be determined."* R12 states similarly that: *"...one of the major problems with blockchain is the connection between the on-chain and the off-chain processes."* Also, R4 explains that: *"You still have to employ some more traditional management controls there. It's often referred to as an "Oracle problem" or a "gateway problem', meaning that you still have to ensure that the container is, in fact, in Burkina Faso and not in Nairobi, Kenya. Just because blockchain says it is there, it doesn't have to mean it is also physically. That is different from Bitcoin and other cryptocurrencies because they only exist within the system and are not connected to physical value."* Looking at off-chain related governance in the networks, there are several types of nodes in a network, such as businesses, service providers, academics, and nonprofits. Organizers must now decide how the network's numerous stakeholder groups will be represented inside it, as well as the structure of its board of directors. There are several crucial problems, including the board's members, how it is elected or appointed, the percentage of votes needed to support a decision, and the qualified majority necessary for a transaction to be undertaken. Blockchain consortium members and other key stakeholders should be represented on the board. Members' service on the board will normally mirror that of the board members' service time. There will be a majority if the board size is sufficient and there are enough stakeholders to give Board decisions legitimacy.

Additionally, the structure of the board and the demand for legality will impact the number of votes each board member casts. Majority votes are typically required for changes in the board's makeup, the allocation of seats among membership classes, and passing a law, among other things. It is the board's responsibility to propose and appoint executive officers who are in control of the consortium's daily operations. Fewer board members from one organization or group of affiliated enterprises are one way many consortia ensure that no one company has an undue amount of control over the group. Finally, even though board approval is often used for routine project decisions, board members may insist on further approval for choices like the approval of the category of members.

5.2 Governance Structure Consortium Blockchain

R4 explains that: *"The governance structure consists of three components of governance: the Governance Board, the Technical Steering Committee, and the Marketing Committee. The 'Governance Board' consists of 21 Premier Members, with one representative nominated by each Premier Member, elected General Member members, and a Chair elected by the Technical Steering Committee."*

The Governing Board of the Hyperledger Foundation is responsible for approving the Foundation's budget, appointing a Chair of the Foundation, approving expenditures, and overseeing any day-to-day activities; overseeing the Foundation's commercial and marketing operations; and establishing and upholding the Foundation's rules and regulations, such as its Code of Conduct, trade regulations, and the Foundation's Bylaws.

Whereas the 'Technical Steering Committee' is made up of fifteen Contributors or Maintainers chosen by Active Contributors. They meet every Thursday, and the dates and times are posted on our community calendar for everyone to see. To the codebase, wiki, and other Hyperledger outputs, contributors submit code and documentation. Maintainers, on the other hand, are Contributors who have been promoted to the level of accepting change requests and uploading new code and updates directly to a project's archive for distribution. Anybody may become a contributor or maintainer to Hyperledger, a nonprofit organization. As a result of this, the TSC is in charge of selecting a TSC Chair, who is also a voting member of the Governing Board and is responsible for serving as a liaison between the Governing Board and the technical leadership of the Hyperledger Foundation. For its final role, the TSC is responsible for overseeing the Hyperledger Foundation's technical direction, approving new projects,

establishing cross-project working groups to address technical issues and opportunities, exchanging information with other organizations, and representing other standards groups; and coordinating with the Hyperledger Foundation's Advisory Board.

Finally, the 'Marketing Committee' consist of one voting representative from each Premier Member, one or more non-voting Maintainers nominated by the TSC, and one or more non-voting representatives. One of the requirements for becoming a maintainer is that the participant must have been active in the community for a while. The Marketing Committee is in charge of coming up with a marketing plan for the Governing Board and putting that strategy into action.

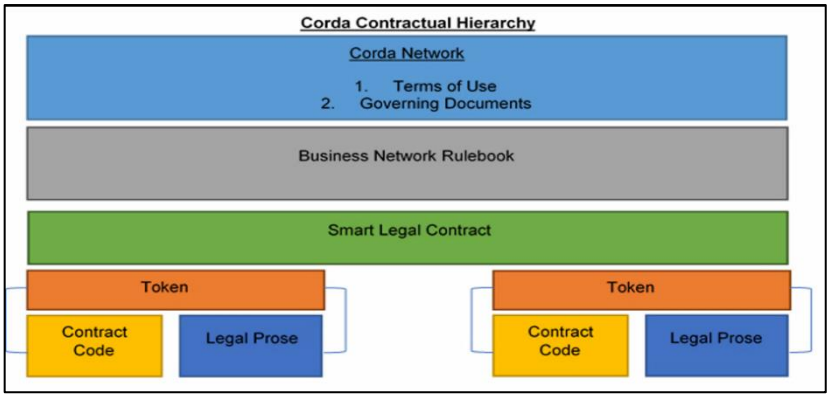
Similarly, R3 has established the Corda Network Foundation, a Dutch nonprofit organization founded in December 2018, which governs the Corda Network. The Corda Network Foundation is a board comprising nine early network adapters, including B3i and Marco Polo, as well as two members from R3, on a nonprofit corporation with no shareholders. Every board member has a vote, and the board is selected in a randomized order by the members themselves. Aside from determining if the network operator is doing well, this also includes determining pricing and scope, as well as laws. The network's safety and efficiency are top priorities, but so is enabling it to grow to its full potential.

Furthermore, the network's root Certificate Authority (CA) serves as a sanctions checker and provides identity certificates to nodes that join; the network's nodes are listed on a map, and the Network Operator or participants themselves can implement the consensus mechanism for nodes to interact over it. Using this technology, transactions between any two nodes in the network are completely frictionless. Legal entities of all kinds, from businesses to nonprofits alike, are making use of it to do business. There is a need for fair and reasonable agreement from all parties to transact business via an irreversible ledger that defines the collective understanding and prevents disagreements from arising. That is why participants rather than shareholders must hold the Foundation's board of directors and voting power. Their role is to help lead and oversee a firm for three years. They are also responsible for ensuring that the Network Operator offers reliable and steady service and that its customers are satisfied. Pricing the network is a word R3 describes as the process of determining a network's participation and transaction fees in order to keep costs low for users. The rest of the network accepts all changes to network characteristics

and system enhancements, and the Foundation's structure, voting method, and standards are followed appropriately. See figure 16.

Figure 16

Corda Contractual Hierarchy

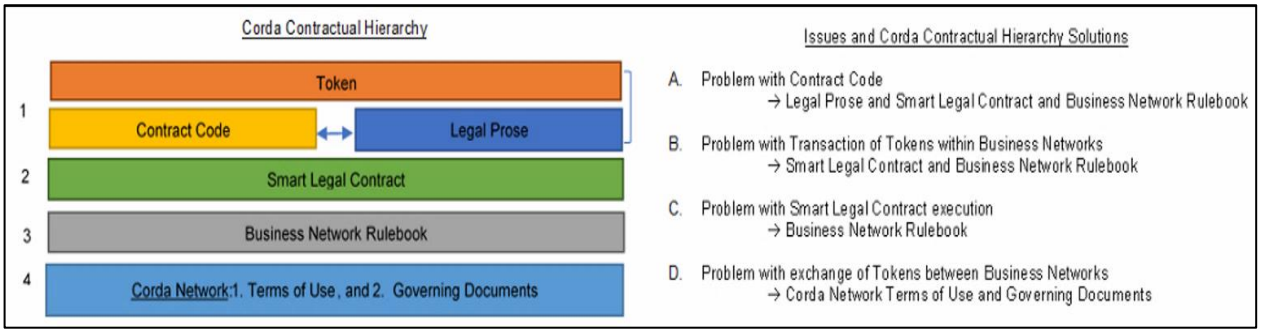


Note. From screenshot during interview respondent 3.

Corda Contractual Hierarchy is the governance framework R3 developed. The design is an example of a 'self-contained governance paradigm,' as the term suggests. Upon guarantee that the parties have signed legally binding contracts and are aware of the processes for resolving disputes if a problem arises, conditions agreed to by the parties interact throughout the process. All legal difficulties must be overcome in order for the model to work. See figure 17.

Figure 17

Corda Contractual Hierarchy



Note. From screenshot during interview with respondent 3.

The structure of the consortium blockchains from the interview findings corresponds with the governance form NAO as mentioned by Provan and Kenis (2008) that can be found in literature around network governance. As mentioned in the literature review, the Network Administrative Organization is a separate administrative organization that governs the network's operations. The NAO is not a member organization delivering its own services but consists of the

network members who are voted network members are for-profit firms, as can be seen by The Corda Network Foundation.

5.3 The Accountable Client Entity

Likewise the accountable client entity should be the governance board who is a separated entity consisting and voted by the consortium members. As mentioned earlier, in the literature this is called the NAO. See figure 14.

6 Design Artifact

In this chapter, background information is given, followed by interview findings of the consortium blockchain providers, the requirements for the artifact given by the IT auditor, the design of the artifact, and the concept standard itself containing the CBAC Framework.

6.1 Background Information

For this artifact, the basis is inspired by the ISAE 3000 used for SOC 2 and SOC 3 reporting. The abbreviation ISAE stands for 'International Standard On Assurance Engagements.' This standard is the guideline for conducting the audit, and this audit is intended to demonstrate that an organization's internal management processes are performed as described. The ISAE 3000 identifies the incremental requirements and guidance when performing examination engagement of the description of a system and the related controls at a service organization following the Trust Service Criteria (TSC) (security, availability, confidentiality, processing integrity, and privacy (EY, n.d.).

With an ISAE 3000, a service organization can demonstrate that they are in control of their services and carrying out the control measures properly. The main stakeholders of the ISAE 3000 are:

- **User organizations/ entity:** An entity that uses a service organization.
- **Service organizations:** an organization or segment that provides services to user entities.
- **Sub-service organizations:** an organization or segment that provides services to the service organization.
- **Service Auditor:** a practitioner who reports on controls at a service organization.
- **User Auditor:** the auditor who audits and reports on the financial statements of a user entity (EY, n.d.).

6.2 **Requirements**

The requirements are a list sent by an IT auditor of EY. Respondent 2 states: "*Keeping in mind risks associated with blockchain platforms and evolving attack vectors with blockchain. It would be nice to have the following control requirements in place:*

- *Pre-implementation - Suitability of DLT platform for the selected use case.*
- *Key ownership and management - Secure storage, maintenance, review, and governance of cryptographic private keys used for authentication and validation by nodes.*
- *Interoperability & Integration - Consistent communication between multiple network participant platforms and enterprise legacy systems.*
- *Consensus Mechanism - Nodes validate blocks in the chain to maintain a single version of the truth to keep adversaries from derailing the system and forking the chain.*
- *Heterogenous regulatory compliance - Compliance with laws and regulations across various countries and state legislations that govern information and transactions processed.*
- *Access & permissions management - Permissions configured for defined roles for access, validation, and authorization of blockchain transactions by internal and external participants.*
- *Network & node governance - Monitoring network for information compliance and node reputation checks to handle and resolve disputes.*
- *Network-Vulnerability Management - The enterprise effectively manages blockchain network vulnerabilities through monitoring, remediation actions, and communication to relevant stakeholders.*
- *Endpoint Security – The enterprise properly manages end-user devices using the blockchain solution (i.e., the end users' devices are tracked, hardened, and addressed if compromised).*
- *Vendor Due Diligence – Due diligence for vendors/suppliers and operational processes ensures ongoing alignment between the enterprise's strategic objectives and DLT solutions.*
- *Business Continuity and Disaster Recovery – Private / permissioned blockchain has centralized and decentralized components. There needs to be a concrete understanding of what will happen should these components be affected by any potential factors.*

- *Transactions - Mechanisms in place to verify and monitor transactions."* (full interview transcripts are included in Appendix A).

6.3 Design

The Consortium Blockchain Audit Control Framework consists of the basic elements: risk, control objectives, control, and control classification; and extra columns like topic, reference to practice and frameworks, and the check by expert. The development of the framework starts with looking at different frameworks limited to COBIT, ISO, and NIST.

Topic

The topic is the theme of the overall process influenced by the stakeholder policies and procedures. It gives each risk, control objective, and corresponding control a brief overview of what the control is about. The topic is based on the theories that were discussed in the literature review. See table 9 for the overview.

Table 9

Alignment theory and topic of the Consortium Blockchain Audit Control Framework

Topic	Theory	Author
Consortium Governance	Network Governance	Provan and Kenis (2008)
Consortium Performance	Smart Business Network	Van Heck and Vervest (2007)
Consortium Regulatory Compliance	x	x
Consortium Businesses Alignment	Extended Strategic Alignment Model	Torabkhani et al. (2007)
Consortium Access Management	Model of Trust	Mayer et al. (1995)
Consortium Auditing	Audit & Assurance Agency Theory	Eisenhardt (1989) AICPA ISACA ISO

Risk

A risk is a situation where a process or activity of an entity is exposed to internal or external danger. This column contains all risks categorized per topic.

Control Objectives (Why)

When conducting an audit, it is important to know what safeguards are anticipated to be in place in order to mitigate any inherent risks that may be present. There must be a clear declaration of the intended outcome or goal in order to address the inherent danger in the subject areas under study in place. Based on the risk and control goals given in the Consortium Blockchain Audit Control Framework, an IT auditor may analyze this information to assess if the review will achieve audit objectives. The format for control objectives is based on that of EY: *"Controls provide reasonable assurance that…[why: subject] maintained in a complete, accurate, and timely manner."*

Controls (What, When, Who, and How)

To achieve the control objective, this field provides a detailed description of the intended control actions. This column contains the controls, which are (consortium) structures and practices that are used to manage risks, such as policies, procedures, guidelines, practices, and network policies. Roles and responsibilities, documentation, forms, reports, system configuration, division of tasks, approval matrices, etc., are all examples of ways to implement control measures in a consortium. The controls can be formulated as in:

- WHAT: What evidence supports the performance of the control?
- WHEN: When is the control performed?
- WHO: Who performs the control?
- HOW: How precise and sensitive is the control?

Control Classification

This column contains the classification of the control. For each control objective, three types of controls are mentioned to indicate the logic from preventive control to the carrying out of mitigating solutions in the corrective control. The classification of controls can be categorized into three categories:

- Preventive controls aim to avert a problem before it arises.
- Detective controls should generate an alert to trigger the corrective controls when a deviated risk is detected.
- Corrective controls should aim to limit the impact of an event and help resume normal operations within a reasonable time frame.

Reference to practice or frameworks

This column refers to standards and/or frameworks that are used in this framework to derive the specific control (e.g., COBIT, NIST, and ISO).

Check by Expert

This column is made to validate the controls by cross-checking these controls with different experts like blockchain experts, consortium blockchain providers, and IT auditors.

6.4 Consortium Blockchain Standard

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal, or other professional advice. Please refer to your advisors for specific advice.

6.4.1 Intro

To offer a general framework and best practices for auditing consortium blockchain, these recommendations have been drafted to give instructions on which domains and aspects of the consortium blockchain should be examined. The purpose of these recommendations is to eventually assist auditors who are conducting audits of consortium blockchain systems and the consortium itself. A wide range of consortiums may benefit from this advice, regardless of size or nature.

6.4.2 Consortium Blockchain Roles

As part of a consortium blockchain, it is necessary to understand the function and roles, and sub-roles of each member as well as the tasks they do. In table 10, the role and sub-role of members are described. Not all consortium blockchains include roles and sub-roles like these. It is also crucial to remember that one consortium member may play several roles and sub-roles at the same time. It is also possible to divide various responsibilities and sub-roles across several consortium members.

Table 10

Consortium Blockchain Roles

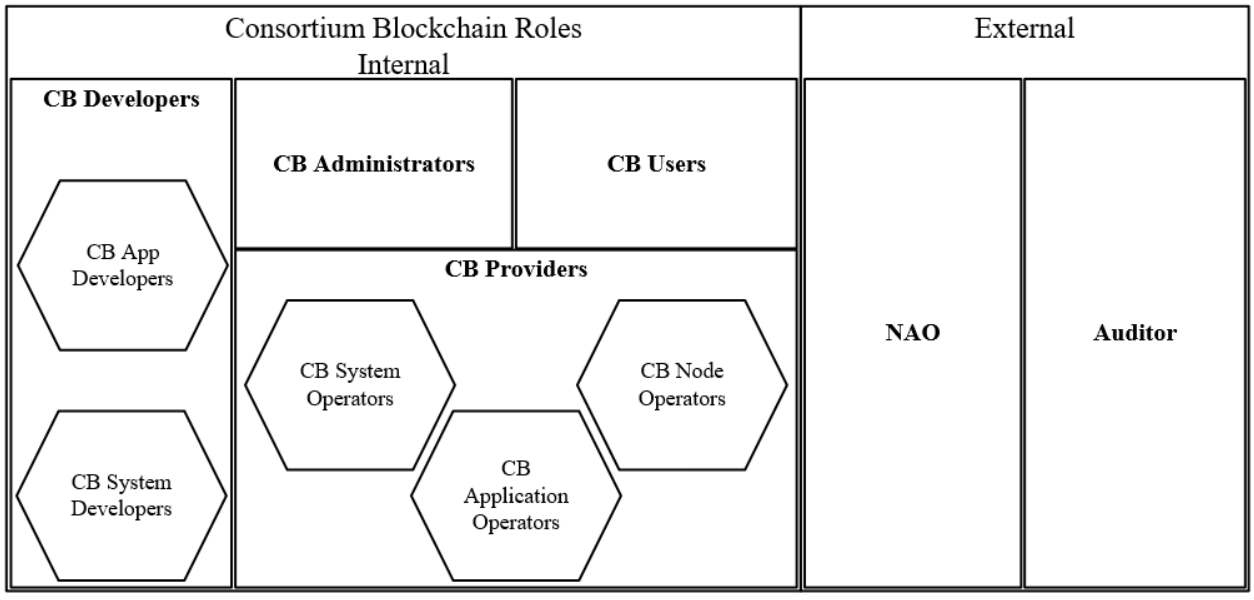
Consortium Blockchain Roles	Description
1. CB Developers:	Code and specialized equipment for any aspect or deployment of CB systems or apps are created and maintained by CB developers. CB Application Developers and CB System Developers are two sub-roles for CB developers.
a. CB Application Developers (for CB users and CB providers)	CB Application Developer creates and manages custom business applications as. The CB system's nodes may also be used to interface with programs outside the system, using a user API provided by the nodes. CB apps may be utilized, hosted, and operated by either CB Users or CB Providers, depending on their needs. Roles and access needs for them must be taken into consideration while developing a CB app. For example, they are creating and maintaining business systems based on CB systems and creating and maintaining components in CB system systems.
b. CB System Developers (for CB providers)	CB System Developers design and build the physical and digital systems that house and operate the CB node components and platforms. A few examples are the development of CB platform components and component testing for node operators and users.
2. CB Administrators	CB Administrators perform a unique administrative function. Depending on the system or network, the responsibilities of administrators may change. CB nodes will be able to act for some, whereas CB solutions will be able to act for others. For example, installing user apps, configuring CB user applications and administration programs, and managing role-based access restrictions are some of the tasks that fall under "managing security policy."
3. CB Users	A CB user uses the CB solution. A CB user can be represented as a human, organization, device, or system may all be represented by this one symbol. CB users use DLT API-based applications and off-ledger code to interface with a CB system rather than directly with a CB node. Users of CB who are automated systems rather than human beings connect with the program using an API provided by CB.
4. CB Providers:	CB Providers can operate the CB system or consortium blockchain. CB providers must agree to create/instantiate nodes, join networks, and pay for and manage contractual agreements to join a network. Sub-roles include CB System Operators, CB Node Operators, and CB Application Operators.
a. CB System Operators	CB System Operators manage and maintain all aspects of the physical and digital systems and networks on which the CB system and platform function in the consortium blockchain. CB System Operator handles the connectivity between nodes, interoperability between nodes, and policy enforcement. In addition to managing the

	CB system's communication networks, the physical and digital systems must be deployed, as well as established environments and procedures.
b. CB Node Operators	CB node operator oversees and manages one or more nodes inside a CB system for a CB provider. CB Node Operators are in charge of all aspects of a node's lifespan, including deployment, operation, management, and maintenance.
c. CB Application Operators	CB Application Operator administers, operates, and maintains CB applications systems to provide CB services for CB users. A CB Application Operator may offer CB services by owning or managing a CB node or by providing CB business services via the CB node owner's service.
External roles	**Description**
5. NAO	The NAO governs the whole consortium blockchain to ensure that nodes can carry out their intended functions. Decentralized systems may need the creation of new governing structures and the flexibility to adapt when circumstances change.
6. Auditor	The auditors verify that the CB complies with policy, governance, and legislation rules. They can collaborate with various stakeholders, including operators, regulators, governors, etc. For example, evidence for an audit must be gathered to meet certain standards, criteria, frameworks, or alternatives.

Note. Adapted from "ISO/FDIS 23257: Blockchain and distributed ledger technologies — Reference architecture," by ISO, 2021, *INTERNATIONAL STANDARD*, p. 29 – 34. Copyright 2021 by ISO.

Figure 18

Consortium Blockchain & external roles and sub-roles



Note. Adapted from "ISO/FDIS 23257: Blockchain and distributed ledger technologies — Reference architecture," by ISO, 2021, *INTERNATIONAL STANDARD*, p. 30. Copyright 2021 by ISO.

6.4.3 CBAC Framework

As respondent 3 states for best practice: *"to determine whether blockchain governance is successful, we should look at its results. For example, the stability, size, and interaction of the users with the network and how key stakeholders are involved in this process."*

For an effective governance framework, intellectual property ownership and license should be provided. Part of which is choosing the right entity, classifying stakeholders, creating visual representations, and reserving voting rights for important topics should all be part of the process. The Consortium Blockchain Audit Control Framework offers management with a comprehensive set of high-level blockchain control objectives that are developed from specific business goals based on the following six risk domains: Governance, Performance, Regulatory Compliance, Businesses Alignment, Access Management, and Auditing. See table 11.

Table 11

Consortium Blockchain Audit Control Framework

Topic	*#*	*Risk*	*Control Objective (Why)*	*Control (What, When, Who, and How)*	*Control Classification*	*Reference to practice or frameworks*
Consortium Governance	1	Missing responsibility / Ownership and Conflict of interest between consortium participants.	CG: Controls provide reasonable assurance that the responsibilities of the blockchain are clearly defined, and the Business Goals and requirements of the consortium are met and maintained in a complete, accurate, and timely manner.	CG-1: Document the roles and responsibilities of the consortium members to have segregation of duties before the implementation of the DLT in the consortium.	Preventive	EY Control
	2			CG-2: Detailed blockchain requirements, specifications as well as policies, and guidelines for the running of the blockchain are documented and approved by the consortium members before the implementation of the DLT.	Detective	COBIT 2019: BAI04.05, DSS05.02, DSS05.03, MEA02.01, MEA04.07 NIST CSF ID.BE-3
	3			CG-3: The NAO assures risk mitigation plans are carried out in the consortium.	Corrective	COBIT 2019: BAI04.05, DSS05.02, DSS05.03, MEA02.01, MEA04.07 NIST CSF ID.BE-4
Consortium Performance	4	The consortium is performing below expectation, or there is no single agreement on goal achievement.	CP: Controls provide reasonable assurance that there is an agreement between consortium members of a fixed value(s) of goal achievement and is maintained in a complete, accurate, and timely manner.	CP-1: The NAO performs a fit-for-purpose assessment to understand the impact of the blockchain being deployed per node and creates and approves an overview of consortium KPIs before the implementation of the DLT based on the collective input of the consortium members to review the progress of the consortium performance.	Preventive	EY Control
	5			CP-2: The NAO tracks the KPIs daily and monitors the progress of the results, and reviews them during monthly meetings.	Detective	EY Control
	6			CP-3: The NAO adjusts the KPIs when necessary to mitigate or minimalize the risks as much as possible during monthly meetings.	Corrective	EY Control

Consortium Regulatory Compliance	7	Non-compliance with legal and regulatory requirements.	CRC: Controls provide reasonable assurance that the consortium blockchain is designed and implemented based on regulatory and legal compliance and is maintained in a complete, accurate, and timely manner.	CRC-1: The NAO assures compliance with privacy standards in the respective jurisdictions where the consortium operates before the implementation of the DLT, e.g., General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Protection of Personal Information Act (POPIA) (South Africa), Brazil's Lei Geral de Proteção de Dados (LGPD), etc.	Preventive	BLOCKCHAIN FRAMEWORK AND GUIDANCE: COBIT 2019: APO01.01, APO01.09 APO13.02, BAI01.07 BAI03.03, BAI03.07 BAI03.08, DSS06.02 MEA03.01 NIST CSF ID.GV-3 ISO/IEC 27001:A.18.1
	8			CRC-2: The NAO reviews regulatory compliance with all jurisdictions impacted by the consortium.	Detective	BLOCKCHAIN FRAMEWORK AND GUIDANCE: - COBIT 2019: BAI09.01, MEA03.01 MEA03.04 - NIST CSF ID.GV-3 - ISO/IEC 27001 A.18.1
	9			CRC-3: The NAO should remove consortium members when the consortium member's regional regulation makes it hard to operate in that region.	Corrective	BLOCKCHAIN FRAMEWORK AND GUIDANCE: COBIT 2019: BAI02.01, MEA03.01 MEA03.04 NIST ID.GV-3 ISO/IEC 27001 A.18.1

Consortium Businesses Alignment	10	Lack of interoperability and scalability between nodes.	CBA: Controls provide reasonable assurance that the scoping purpose of the consortium blockchain is formally defined, and the scalability and interoperability between the nodes are aligned and maintained in a complete, accurate, and timely manner.	CBA-1: The NAO ensures that the business operation layer and platform formats align with standards (voluntary or required) to enable desired interoperability between consortium members.	Preventive	BLOCKCHAIN FRAMEWORK AND GUIDANCE: COBIT 2019: APO14.02, BAI03.03, BAI03.08
	11			CBA-2: The NAO performs an annual capabilities assessment of the requirements to scale the blockchain in the current business alignment and reviews it quarterly.	Detective	EY Control
	12			CBA-3: The NAO adjusts the scoping definition annually and approves it by every consortium member.	Corrective	EY Control
Consortium Access Management	13	Disclosure and access to confidential transactions, contractual and information of the consortium, and unauthorized logical access to blockchain systems causing service disruption, lack of availability, integrity, or confidentiality.	CAM: Controls provide reasonable assurance that node/consortium access and validation are ensured and maintained in a complete, accurate, and timely manner.	CAM-1: The NAO and the consortium member(s) protect the consortium from access by unauthorized nodes in the private consortium.	Preventive	BLOCKCHAIN FRAMEWORK AND GUIDANCE: COBIT 2019: APO13.01, DSS01.04, DSS05.03 NIST CSF PR.MA-2, DE.CM-7, PR.AC-3 ISO/IEC 27001:2013 A.13.1, A.13.2

	14			CAM-2: The NAO assures appropriate know-your-customer (KYC) and anti-money laundering (AML) screening on exchanges and other on-ramps to the consortium blockchain.	Detective	BLOCKCHAIN FRAMEWORK AND GUIDANCE: COBIT 2019: DSS06.02, MEA03.04 NIST CSF PR.DS-6, DE.DP-2, ID.GV-3 ISO/IEC 27001:2013 A.18 B3i Interview
	15			CAM-3: The NAO ensures that inactive or ex-users/members are terminated from accessing any transactions on the consortium blockchain	Corrective	BLOCKCHAIN FRAMEWORK AND GUIDANCE: COBIT 2019: DSS05.04, DSS06.03 NIST CSF PR.AC-1 ISO/IEC 27001:2013 A.9.2.1
Consortium Auditing	16	Disclosure and access to confidential transactions, contracts, and information of the consortium.	CA: Controls provide reasonable assurance that a comprehensive audit and monitoring of the DLT are maintained in a complete, accurate, and timely manner.	CA-1: The NAO sets an appropriate minimal limit of members to assure that no single node or group of nodes controls an inappropriate percentage of the consensus or consortium resources at any time.	Preventive	BLOCKCHAIN FRAMEWORK AND GUIDANCE: COBIT 2019: EDM01.03, MEA01.01, MEA02.01 NIST CSF PR.PT-1 ISO/IEC 27001:2013 A.12.4, A.12.7
	17			CA-2: The NAO establishes and confirms that there is an integrated audit/monitoring process in regards to the DLT supported by service organization control (SOC) reviews.	Detective	BLOCKCHAIN FRAMEWORK AND GUIDANCE: COBIT 2019: APO14.05, APO14.06, BAI03.02 NIST CSF ID.AM-4, DE.CM-6

						ISO/IEC 27001:2013 A.14.2
	18			CA-3: The NAO removes inactive or ex-users as soon as possible.	Corrective	BLOCKCHAIN FRAMEWORK AND GUIDANCE: COBIT 2019: BAI02.01, DSS05.04, DSS05.07, DSS06.03, MEA03.01 NIST CSF ID.GV-3 ISO/IEC 27001:2013 A.18

7 Evaluation

This chapter is a compilation of the most significant findings from the evaluation phase interviews R9 – R12, which is done in an iterative process as mentioned in chapter 4.6, 'Research Process.'

7.1 Evaluation

The interview results are organized according to central feedback points from the respondents. Annotated excerpts from the interview transcripts (Appendix A) are used to illustrate the results. The names of respondents have been replaced with numbers in order to maintain anonymity. The abbreviation 'R#' stands for 'Respondent #.' The feedback points from the interview findings are:

1. Ordering of the columns
2. The addition of corrective controls to the framework
3. Merging of Topics
4. Preventive, detective, and corrective controls per topic
5. Numbering of controls
6. A standard formulation for control objectives and containing the 'why' attribute
7. Containing the what, when, who, and how attributes for controls

1. Ordering of the columns

One of the feedback points on the structure of the framework is about the ordering of the columns (R9), (R10), and (R11). The structure of the columns was first: topic, control objectives, control, risk, and control classification. Based on R9, their feedback states: *"Normally you identify the most critical risks based on your control objectives and controls on those risks. That would be an approach that we also know and use."* After that, this feedback point was cross-checked with R10, which states: *"I also have a control framework from one of our clients. We have the TSP, which in your case, is the topic. I am going to cross-check the columns for you. You mention the theme, risk control objectives, the control itself, description, and control classification. It seems you mention them all." Afterward, the feedback is cross-checked with R11, which mentions: "The setup is good." Finally, R12 states: "There are certain specific risks formulated by EY worldwide that are mentioned in the global audit methodology. And those risks are always like the starting points for basically everything. Every risk applies to every situation*

and organization, but it is a starting point. So I would say this is the correct order. So you did it correctly, in my opinion."

2. The addition of corrective controls to the framework

R9 states: "…*the combination of at least preventive and corrective is the key to a good framework."* R9: *"many companies have a scanner in place to detect specific intrusions, for example. But if they don't follow up, for example, such management or another type of corrective action, they detect, but they never fix it. I think that's why you need the combination of those types of controls because the section alone of the vulnerability like that doesn't really make a difference. So then, it's really good to have the combination of detection and to act upon detecting mistakes or things that happen. So I think it might be an essential improvement if you mentioned the corrective controls."* As well, R10 states a similar statement: **"***Indeed, actually, for every audit, it doesn't matter if it's a financial IT operation or cyber audit or something. You always have preventive, detective, and corrective controls."*

3. Merging of Topics

A third feedback point that is implemented is the merging of some topics into one topic. R9 states: *"I think I think maybe the network ones can be combined into one. And I think they are all separated potentially. You might see them in one primary topic called infrastructure, for example. And then it's divided into smaller ones for those regulatory ones."*

4. Preventive, detective, and corrective controls per topic

One suggestion that was discussed with R9 was to have preventive, detective, and corrective controls per topic to give more an example logic for future researchers of IT auditors to develop the CBAC Framework further. R9 states: *"It's a great approach, but it's not always possible to have all three. It also depends on the topic's importance. But it is possible. Also is one of those controls that fail. Then you have two other controls to remain. So then, if your preventative control fails, you can still do a good job if you detect and correct the errors."* A similar statement is said by R11: *"we often suggest, clients adding more than one control goes for one control objective. Because if you filled this control, for example, on line two, you would not achieve control objectives. There's nothing left there, no other control that will mitigate the same risk or that could help mitigate that risk. So what we often will set for our clients is, if you have one control, try to change it into a preventive and a detective control So if you, for example, fail the first control, that will fill the second control. So there is no review performed, but at least you*

could see that authorizations have been assigned under the procedure or authorizations are revoked in line with the procedure. Then the risk might be minimal of that failing control. You could still achieve the control objective." For that reason this feedback is implemented.

5. Numbering of controls

The fifth improvement is the numbering of the controls. R10 states: **"**Within EY, we have frameworks to send to the client that looks quite similar to this one. Those also use more numeric structuring and reference. So maybe you can put that also in your framework. Kind of a numeric reference, but overall it's quite the same for you. We also have a Framework from the IT audit group NOREA." R10 furthermore shows an example (see figure…) and states: *"You can also give a topic and then a number like A1 or the first control of topic Consortium Regulatory Compliance as CRC-1. As you see, this framework numbers their control in combination with a letter.* In the CBAC Framework (see chapter 5.4.3) the controls are characterized with the abbreviation of the topic followed by a '-#number'.

Figure 19

Example Audit Framework of respondent 10

	A	B	C	D	E	F
1	TSP Category	Trust Service Criteria #	Trust Service Criteria description	Control #	Control Description (2022)	Unique / Referral Control
6	Additional Criteria for Availability	A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	A1.2 - control B	Interxion has defined a Group Maintenance Policy for the environmental protections in the data centre and contains a specification of the assets and their criticality, which are subject to planned maintenance. In principal environmental protections receive maintenance on at least an annual basis, however for assets which are subject to condition-based maintenance other maintenance frequencies may apply in accordance with the Group Maintenance Policy and supplier requirements.	Unique
7	Additional Criteria for Availability	A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	A1.2 - control C	Every data centre facility has 24/365 alarm monitoring (Building / DC Monitoring Systems – BMS / DCMS) in place for environmental threats (power supply failures, fire, water leakage hazards, temperature and humidity monitoring) and is monitored by the local Operations team. In addition to the local monitoring, ECSC logs and monitors 24/7 environmental alarms received on the Group Critical Alarm Platform (GCAP) for all Interxion entities to ensure timely response and communication with customers and stakeholders.	Unique
8	Additional Criteria for Availability	A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	A1.2 - control D	For all Busisness critical IT infrastructure, organisation shall take full and incremental back-ups according to approved back-up procedure. The back-ups shall be monitored and after 5 continious back-up failures in one set there shall be an investigation and remediation performed and documented.	Unique
9	Additional Criteria for Availability	A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A1.3 - control A	Disaster recovery personnel perform an annual test of the recovery plan procedures to determine any gaps in capability to meet availability commitments and system requirements.	Unique
10	Control Environment	CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CC1.1 - control A	Personnel are required to read and accept the set of rules outlining the responsibilities and ethics and the statement of confidentiality and privacy practices upon their hire and to formally reaffirm them (at least) annually thereafter.	Unique
	[illegible]	[illegible]	COSO Principle 1: The entity demonstrates a commitment to	[illegible]	Hiring procedures include background checks or reference validation, which are	[illegible]

Note. From screenshot during interview respondent 10.

6. Standard formulation for control objectives and containing the 'why' attribute

The sixth feedback point that is implemented is the reformulating of control objectives based on a format that R11 provided: *"As for the control objectives they look more like controls. There is also a standard format for formulating control objectives that you can use. It is as follow: "Controls provide reasonable assurance that…[why: subject] maintained in a complete, accurate, and timely manner." "* R11 elaborates, that reason being "*Control objectives are more a higher level."*

7. Containing the what, when, who, how attributes for controls

The final feedback point that is implemented is about the containment of what, when, who, and how in a control statement. R9 states: *One thing I know is maybe how we at the SOCR team want to see control because we're usually pretty critical with our clients and how they formulate things. So it has to be clear what we're talking about, who is performing the process, and the frequency with which it's performed. I think it's in the playbook of what should be in a good control description. Maybe you can put that framework next to your control descriptions and see if your missing something. This should be in the control to make it more clear for the people performing the controls. So there are a few things that may help improve your framework a bit more, but I think it is already good*.

Similarly, R11 explains: *"You can use the WHY, WHAT, WHEN, WHO, and HOW formulation. Well, the "WHY" is clear. You do that to achieve the objective, to mitigate the risk. So that's clear. But you can also apply "WHAT," "WHEN," "WHO," and "HOW" to the control. So you could say in control, what do they need to perform when so if you say, well, a review needs to be performed, analysis needs to be performed, or an assessment is performed, that's also based on the risk assessment. Well, how often do they need to perform that? The monthly is the yearly as is the yearly enough. Maybe you say it's a high risk, so you need to do it at least monthly. And also, who does need to perform the control? So it also helps identify this responsibility of the person in that the organization and what the controls they need to perform."*

8 Communication

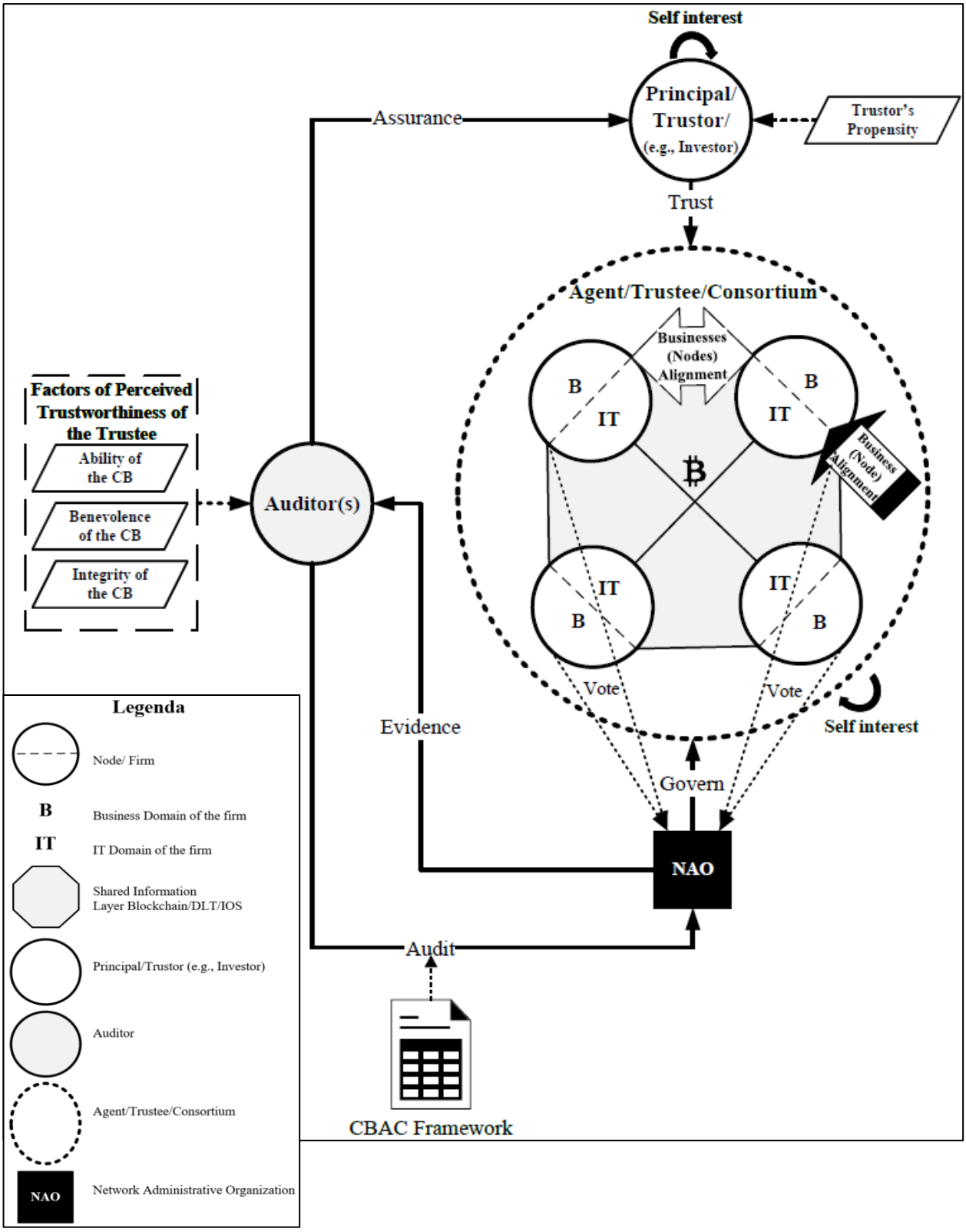
This chapter is the final phase of the DSR. In this chapter, the conclusion of the applicability of the framework is discussed, followed by a recommendation, contribution, and limitation & future research, with finally, this being handed over to EY.

8.1 Conclusion

This study started with the necessity (growth of blockchain business) and lack of availability of standards for consortium blockchain for IT auditors. In order to know "How should an IT auditor audit a consortium blockchain(s)?" this research aimed to take the first step towards improving the auditability of consortium blockchain by making available a concept principle-based IT audit standard that satisfies auditability, control, and governability requirements to help IT auditors audit consortium blockchain(s). As a result of the literature review research, the ABC model is created to give a holistic view of stakeholders and the relationship between the investors or shareholders (principal/trustor), the consortium blockchain client (agent/trustee), and the external auditor (control mechanism) of the consortium blockchain. Based on the prerequisites from the IT auditor and interviews with three consortium blockchain providers, it becomes clear that there is a specifically a lack of off-chain governance (also concluded from the literature review) instead of on-chain governance of whom the CBAC (Consortium Blockchain Audit Control) Framework is developed following blockchain expert's review, which takes a principle-based approach, meaning that the norms are flexible and resting primarily on the professional judgment and knowledge of the IT auditor. The CBAC Framework is evaluated based on four evaluation interviews with IT auditors to cross-check the validity. Based on the CBAC Framework, the IT auditor is supposed to audit the NAO who represents the consortium and is therefore also the accountable client. This holistic view can be seen in the complete ABC model in figure 20. As of now, the concept framework meets the requirements as stated by the IT auditor, and as part of the final DRS phase, the CBAC Framework is given to the IT auditor, who could develop the framework further.

Figure 20

Complete ABC (Auditability Blockchain Consortium) Model



8.2 Recommendation

As a first step toward a fully developed and relevant framework, the CBAC Framework is a good starting point. The External auditors might use this framework to have a better idea of the big picture and learn from its proven procedures. As the leading standards body, ISO should give guidance on domains and audit methods that should be implemented to guarantee that IT risks and business system performance are appropriately controlled in the consortium. The proposed CBAC Framework would include a list of domains to be audited, as well as a list of possible audit controls to guarantee that consortium blockchains are properly audited.

Since the CBAC Framework is principle-based and therefore heavily relies on the professional judgment of the IT auditor, the IT auditor must be up to date with expertise around the topic of blockchain. Within EY there are, therefore, training and workshops that can be followed and badges that can be earned.

8.3 Contribution to Theory and Practice

This research, and in particular the CBAC Framework, sets the first step towards an audit standard from consortium blockchain. As mentioned earlier, there have been no previous studies that particularly show audit standards for auditing consortium blockchain. Respondent 4 states that the problem why it takes so long also for these standards to be developed is that through time the topic got complicated, and the blockchain from the commercial perspective would bend into wherever the money would go, and therefore the taxonomy was not developed at all.

As for EY, the CBAC Framework is handed over to a blockchain expert and IT auditor (respondent 12) with anticipation that they will build the framework further.

8.4 Limitations & Future Research

For this study, limited research was available on types of blockchain consortiums business-focused, technology-focused, and dual-focused. Also, due to limited time, only IT auditors from EY were interviewed instead of a spread between the remaining Big Four companies, Deloitte, KMPG, and PwC. In future research, it would be relevant to study the following points further:

- The concept standard should be built, further developed, and tested. This could be done in cooperation with NEN. Eventually, procedures and guidelines can be followed up.

- Further research could be done around the suitability of the standard for Private & Public blockchain.
- The possible impact that auditing consortiums have on the role of the IT auditor.
- The oracle or middleware between on-chain and off-chain. How do we assure that what happens on the on-chain (what happens on the blockchain) aligns with what happens on the off-chain (everything that is not on the blockchain: can be either physical or digital).

References

AICPA. (2013). Assurance Services: A White Paper for Providers and Users of Business Information. https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/asec_wp_providers_users_bi.pdf

AICPA. (2020). *Implications of the Use of Blockchain in SOC for Service Organization Examinations*.

Alsunaidi, S. J., & Alhaidari, F. A. (2019). A survey of consensus algorithms for blockchain technology. 2019 International Conference on Computer and Information Sciences (ICCIS),

Alt, R., & Smits, M. (2007). Networkability of organizations and business networks.

Audit Quality. (2005). Agency Theory and the Role of the Audit. *London: The Institute of Chartered Accountants in England and Wales*.

B3i. (2021). How B3i Re Creates Business Value Within Reinsurance Contract Administration.

B3i. (n.d.-a). *CLIMATE RISK MODELLING*. https://b3i.tech/climate-risk-models/

B3i. (n.d.-b). *EURAPCO UNITY*. https://b3i.tech/eurapco-untiy/

B3i. (n.d.-c). *FLUIDITY*. https://b3i.tech/fluidity/

B3i. (n.d.-d). *HELP SHAPE THE MARKET*. https://b3i.tech/mga/

B3i. (n.d.-e). *NUCLEAR POOLS*. https://b3i.tech/pools/

B3i. (n.d.-f). *WHAT IS B3I RE?* https://b3i.tech/b3i-re/

Barringer, B. R., & Harrison, J. S. (2000). Walking a tightrope: Creating value through interorganizational relationships. *Journal of management*, *26*(3), 367-403.

Blummer, T., Sean, M., & Cachin, C. (2018). An introduction to hyperledger. *Hyperledger Organization: San Francisco, CA, USA*.

Brewton, P., & Millward, L. (2001). Organizational research methods. In: London: Sage.

Brown, R. G. (2021). Conclave: An Introduction. *R3 CEV*.

Brown, R. G., Carlyle, J., Grigg, I., & Hearn, M. (2016). Corda: An introduction. *R3 CEV, August*, *1*(15), 14.

Browne, R., & Sigalos, M. (2022). Bitcoin investors are panicking as a controversial crypto experiment unravels. *CNBC*. https://www.cnbc.com/2022/05/10/bitcoin-btc-investors-panic-as-terrausd-ust-sinks-below-1-peg.html

Burgemeestre, B., Hulstijn, J., & Tan, Y.-H. (2009). Rule-based versus principle-based regulatory compliance. In *Legal Knowledge and Information Systems* (pp. 37-46). IOS Press.

Clark, T. H., & Lee, H. G. (2000). Performance, interdependence and coordination in business‐to‐business electronic commerce and supply chain management. *Information Technology and Management*, *1*(1), 85-105.

Colbert, J. L., & Jahera Jr, J. S. (1988). The role of the audit and agency theory. *Journal of Applied Business Research (JABR)*, *4*(2), 7-12.

Corda Network. (n.d.). https://corda.network/corda-network-foundation/about-the-foundation

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, *31*(3), 5-21. https://doi.org/https://doi.org/10.2308/isys-51804

DAVIS, D., & Cosenza, R. M. (2005). *BUSINESS RESEARCH FOR DECISION MAKING/DUANE DAVIS AND ROBERT M. COSENZA*.

Deloitte. (n.d.-a). *IT Audit and Information System Security*. https://www2.deloitte.com/me/en/pages/technology/solutions/it_audit_and_information_system_security_deloitte_montenegro_technology_services_solutions.html

Deloitte. (n.d.-b). *What is Assurance?* https://www2.deloitte.com/mt/en/pages/audit/articles/mt-what-is-assurance.html

Dutta, A., Roy, R., & Seetharaman, P. (2022). An assimilation maturity model for IT governance and auditing. *Information & Management*, *59*(1), 103569. https://doi.org/https://doi.org/10.1016/j.im.2021.103569

Dzuranin, A. C., & Mălăescu, I. (2016). The current state and future direction of IT audit: Challenges and opportunities. *Journal of Information Systems*, *30*(1), 7-20.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of management review*, *14*(1), 57-74.

Fijneman, R. (2006). IT-auditor is meer dan controleur van informatietechnologie. *Maandblad voor Accountancy en Bedrijfseconomie*.

Freeman, R. E., & Evan, W. M. (1990). Corporate governance: A stakeholder interpretation. *Journal of behavioral economics*, *19*(4), 337-359.
Gauthier, M. P., & Brender, N. (2021). How do the current auditing standards fit the emergent use of blockchain? *Managerial auditing journal*.
Genesis Block. (2020). *Blockchain 101: What are Blockchain Consortiums?* https://genesisblockhk.com/what-are-blockchain-consortiums/
Gregor, S. (2006). The nature of theory in information systems. *MIS quarterly*, 611-642.
Halterman, C., Winkler, P., & Houtekamer, D. (2021). *Service Organization Control Reporting Event*.
Hearn, M., & Brown, R. G. (2019). Corda: A distributed ledger. *Corda Technical White Paper*.
Hepp, T., Sharinghousen, M., Ehret, P., Schoenhals, A., & Gipp, B. (2018). On-chain vs. off-chain storage for supply-and blockchain integration. *it-Information Technology*, *60*(5-6), 283-291.
Hern, A. (2022). TerraUSD 'stablecoin' delisted from crypto exchanges. *The Guardian*. https://www.theguardian.com/technology/2022/may/13/terrausd-stablecoin-crypto-exchanges
Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 75-105.
Hileman, G., & Rauchs, M. (2017). 2017 global blockchain benchmarking study. *Available at SSRN 3040224*.
Hulstijn, J., Hofman, W., Zomer, G., & Tan, Y.-H. (2016). Towards trusted trade-lanes. International Conference on Electronic Government,
Hyperledger Foundation. (n.d.-a). *About Hyperledger Foundation*. https://www.hyperledger.org/about
Hyperledger Foundation. (n.d.-b). *Distributed Ledgers*. https://www.hyperledger.org/use/distributed-ledgers
Jensen, M., & Meckling, W. (1976). Theory of the Firm: Managerial Behavior, Agency Costs, and Capital Structure. *Journal of Financial Economics*, *3*, 305-360.
Kellerer, W. (1998). Dienstarchitekturen in der Telekommunikation-Evolution, methoden und vergleich. *Technical Report TUM-LKN-TR-9801. 1998*.
Kessler, G. C. (2003). An overview of cryptography.
Le Borne, F., Treat, D., Dimidschstein, F., & Brodersen, C. (2017). SWIFT on distributed ledger technologies: Delivering an industry-standard platform through community collaboration. In: Retrieved September 24th.
Linder, S., & Foss, N. J. (2013). Agency theory. *Available at SSRN 2255895*.
Liu, X., Farahani, B., & Firouzi, F. (2020). Distributed ledger technology. In *Intelligent Internet of Things* (pp. 393-431). Springer.
Locke, L. F., Spirduso, W. W., & Silverman, S. J. (2013). *Proposals that work: A guide for planning dissertations and grant proposals.* Sage Publications.
Luftman, J. N. (1996). *Competing in the Information Age : Strategic Alignment in Practice*. Oxford Scholarship Online. http://www.myilibrary.com?id=44163
http://www.myilibrary.com?id=44163&ref=toc
Maxwell, J. A. (2012). *Qualitative research design: An interactive approach*. Sage publications.
Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, *20*(3), 709-734.
Nathan, J., & Jacobs, B. (2020). Blockchain consortium networks: Adding security and trust in financial services. *Journal of Corporate Accounting & Finance*, *31*(2), 29-33.
Nóbrega, T., Pires, C. E. S., & Nascimento, D. C. (2021). Blockchain-based privacy-preserving record linkage: enhancing data privacy in an untrusted environment. *Information Systems*, *102*, 101826.
Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45-77.
Provan, K. G., Fish, A., & Sydow, J. (2007). Interorganizational networks at the network level: A review of the empirical literature on whole networks. *Journal of management*, *33*(3), 479-516.
Provan, K. G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of public administration research and theory*, *18*(2), 229-252.
R3. (n.d.). *Delivering digital trust for a digital economy*. https://www.r3.com/about/
Rebello, G. A. F., Camilo, G. F., Guimarães, L. C., de Souza, L. A. C., & Duarte, O. C. M. (2020). On the security and performance of proof-based consensus protocols. 2020 4Th conference on cloud and internet of things (CIot),
Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., Cubillos Vélez, A., & Orgad, L. (2021). Now the code runs itself: On-chain and off-chain governance of blockchain technologies. *Topoi*, *40*(4), 821-831.

Ring, P. S., & Van de Ven, A. H. (1994). Developmental processes of cooperative interorganizational relationships. *Academy of management review*, *19*(1), 90-118.
Roberts, H. (2022). *B3i Introduction*.
Romney, M. B., & Steinbart, P. J. (2015). Accounting information systems 13th edition. *UK: Pearson Educated Limited*.
Ross, S. A. (1973). The economic theory of agency: The principal's problem. *The American economic review*, *63*(2), 134-139.
Schilder, A. (2008). Rule-based versus principle-based: Het perspectief van de toezichthouder. *A. de Bos, P. Coebergh & H. van Olden (red.), Regels voor de toekomst. Kansen voor duurzaam ondernemend Nederland, Schiedam: Scriptum*.
Schollmeier, R. (2001). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. Proceedings First International Conference on Peer-to-Peer Computing,
Silvoso, J. A. (1972). Report of the committee on basic auditing concepts. *The accounting review*, *47*, 15-74.
Smits, M. (2002). Performance and development of electronic business networks. *Innovative Business Models in the network economy*.
Smits, M., & Hulstijn, J. (2020). Blockchain applications and institutional trust. *Frontiers in Blockchain*, *3*, 5.
Smits, M., Weigand, H., De Kruijf, J., & Jerom, D. V. (2018). *How Blockchain technology affects performance of financial services* Digital Transformation,
Steinfield, C., Markus, M. L., & Wigand, R. T. (2011). Through a glass clearly: standards, architecture, and process transparency in global supply chains. *Journal of management information systems*, *28*(2), 75-108.
Straub, D., Rai, A., & Klein, R. (2004). Measuring firm performance at the network level: A nomology of the business impact of digital supply networks. *Journal of management information systems*, *21*(1), 83-114.
Taherdoost, H. (2016). Sampling methods in research methodology; how to choose a sampling technique for research. *How to Choose a Sampling Technique for Research (April 10, 2016)*.
Torabkhani, R., Smits, M., & van der Pijl, G. (2007). Improving the performance of business networks in E-government. *BLED 2007 Proceedings*, 54.
Van Heck, E., & Vervest, P. (2007). Smart business networks: how the network wins. *Communications of the ACM*, *50*(6), 28-37.
Vervest, P., Van Heck, E., Preiss, K., & Pau, L. (2004). Introduction to smart business networks. In (Vol. 19, pp. 225-227): SAGE Publications Sage UK: London, England.
Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F.-Y. (2018). An overview of smart contract: architecture, applications, and future trends. 2018 IEEE Intelligent Vehicles Symposium (IV),
Weigand, H., Blums, I., & de Kruijff, J. (2020). Shared ledger accounting—implementing the economic exchange pattern. *Information Systems*, *90*, 101437.
Wieringa, R. J. (2014). *Design science methodology for information systems and software engineering*. Springer.
Williams, I. (2020). *Contemporary Applications of Actor Network Theory*. Springer Nature.
Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.
Zheng, Z., Dai, H.-N., & Wu, J. (2021). *Blockchain Intelligence: Methods, Applications and Challenges*. Springer.
Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE international congress on big data (BigData congress),

Appendices

Appendix A: Interview Transcripts

Respondent 1: Employee from NEN

No recordings available (based on screenshots, links being shared and note taking during interviews)

I: What is the process for developing a standard within the NEN organization?

R1: Within NEN, we work with the standards committee responsible for the particular standard. We explain to the participant the standard development process and how they can participate in contributing their ideas about a standard and making agreements with stakeholders in their field. Within NEN, we have the seven steps of standard development:

We start with the 'Proposal phase,' where we look for what kind of product or service the development of a joint agreement is important.

In the 'Preparation phase,' we look at what the standard does help with. For example, which problem does a joint agreement offer a tool for? What is the purpose of the joint agreement? Who has the knowledge and expertise in this area? Which parties have an interest in this?

Then in the third phase, we select members of the standards committee. Standards committees are set up for specific standardization activities. Participation in a standards committee is open to knowledgeable members. These members represent the interests of stakeholders of the subject in question. Usually, these parties are producers, traders, users, governments, or consumer organizations. NEN and the stakeholders overview the organizations interested in the new standard. The goal is 'all parties concerned. A result is a broad group of stakeholders representing the relevant sector. Stakeholders can participate in the development of the standard. It is therefore not an obligation to participate in the standards committee.

Then we have the 'Develop Standard phase.' In this phase, standards are drawn up in the standards committees. NEN supervises the process; experts provide the knowledge. By participating, stakeholders influence the content of the standard. A standard is established based on consensus.

In the fifth phase, we are going to publish the initial draft. Market parties can provide input, and the standards committee processes the comments. Afterward, the final product is

published. In the sixth phase, anyone can view and use the standard via the NEN website. NEN announces in press releases, among other things, that the standard has been published.

Finally, in the seventh and final phase, the developments in the market are discussed in standards committees. Standards committees discuss experiences with the standard and include suggestions for improvements in a new standard version. If the members agree, the developments will be included in revising the standard.

In most cases, NEN follows the ISO. ISO begins its process by developing a draft that addresses a particular market requirement. Comments and additional debate are solicited on this draft before it is released to the public. Consensus can only be achieved via a voting process with the draft on its way to becoming an ISO standard if that goal is met. The document will be reworked and voted on until consensus is obtained. Like NEN, ISO does not decide when to develop a new standard. It is built based on requests and needs from standards from the industry by specialists from across the globe who work together in bigger groupings called technical committees to create ISO standards. These specialists negotiate the standard's scope, major definitions, and content. In addition to industry specialists, the technical committees include representatives from consumer groups, academics, non-profits, and the government. The ISO standard-setting process is based on consensus and considers input from many stakeholders.

I: How long does the development process of a standard take?

R1: Developing a standard normally takes around three years from the initial proposal to publication.

I: Are there any developments regarding Blockchain auditing standards?

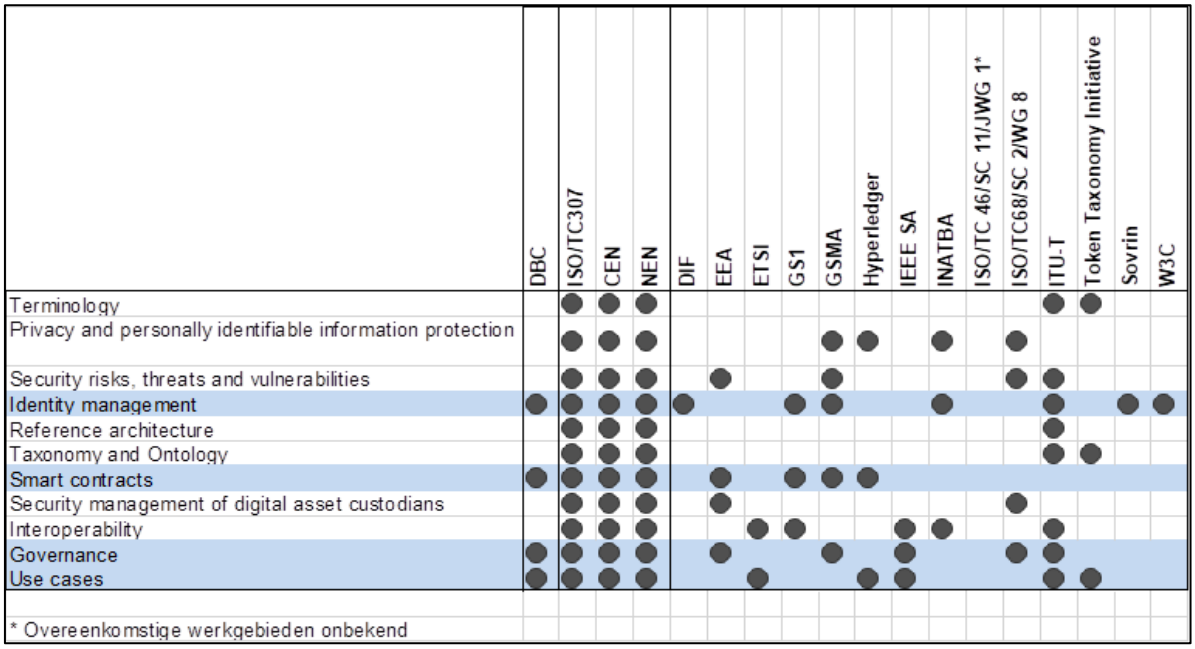
R1: In the field of blockchain auditing, an ad hoc group was established in 2020 (ISO/TC 307/AHG 2 Guidance for Auditing DLT Systems). Ten countries indicated that they would like to provide experts for this. This providing means that there was sufficiently broad international interest in the subject. However, the project is currently largely on hold due to a lack of project management. This lack of project management can change when someone takes the initiative to revive the subject. NEN can support EY in initiating new standardization projects around

blockchain auditing. EY can also participate in ISO groups via the NEN blockchain standards committee. At the moment, there is little that can be done with which EY can join.

The primary goal of TC307's work is to provide standards for DLT-based system installation, risk detection, and governance. Though they give important recommendations, other ISO standards like ISO 27001.2013, ISO/IEC 27017, ISO/IEC19011:2011 do not address the unique challenges of DLT technology adoption or the risks involved. In order to guarantee that DLT-based systems are properly audited, a proposed guidance note would specify the domains to be audited and offer possible approaches.

Figure 21

Comparison between Standards Development Organizations (SDO)



Note. From table sent by respondent 1.

Respondent 2: Blockchain expert at EY (I)

NOTE: No record available at the time due to EY Privacy measures and Team recording restrictions. The list is based on the requirements mailed after the interview due to limited notes taken during the interview.

I: What are important requirements you want to see in a standard for consortium blockchain?

R2: Keeping in mind risks associated with blockchain platforms and evolving attack vectors with blockchain. It would be nice to have the following control requirements in place:

- Pre-implementation - Suitability of DLT platform for the selected use case.
- Key ownership and management - Secure storage, maintenance, review, and governance of cryptographic private keys used for authentication and validation by nodes.
- Interoperability & Integration - Consistent communication between multiple network participant platforms and enterprise legacy systems.
- Consensus Mechanism - Nodes validate blocks in the chain to maintain a single version of the truth to keep adversaries from derailing the system and forking the chain.
- Regulatory compliance - Compliance with laws and regulations across various countries and state legislations that govern information and transactions processed.
- Access & permissions management - Permissions configured for defined roles for access, validation, and authorization of blockchain transactions by internal and external participants.
- Network & node governance - Monitoring network for information compliance and node reputation checks to handle and resolve disputes.
- Network-Vulnerability Management - The enterprise effectively manages blockchain network vulnerabilities through monitoring, remediation actions, and communication to relevant stakeholders.
- Endpoint Security – The enterprise properly manages end-user devices using the blockchain solution (i.e., the end users' devices are tracked, hardened, and addressed if compromised).

- Vendor Due Diligence – Due diligence for vendors/suppliers and operational processes ensures ongoing alignment between the enterprise's strategic objectives and DLT solutions.
- Business Continuity and Disaster Recovery – Private / permissioned blockchain has centralized and decentralized components. There needs to be a concrete understanding of what will happen should these components be affected by any potential factors.
- Transactions - Mechanisms in place to verify and monitor transactions.

To ensure system design and stability, certain users may need assurance that the blockchain service (private /permissioned) or the new platform they are moving to is safe and secure. Users have the option to do their research. But DLT features should be built to consider advanced ITGCs that guarantee proactive security for sensitive information, integrity, availability, and confidentiality. For a private DLT to be successful over the long run, an impartial, trustworthy third party must certify that the controls are functional. Thats where we come into play. There are several advantages to using a trustworthy third party as an access-granting authority for permissioned distributed ledger technology (DLT). Before giving access to the DLT systems, a the audit party will be in charge of performing identity checks and authenticating users' credentials. It may also enforce and monitor the blockchain protocol for security reasons. When a node hosts this service, the confidence among other nodes decreases. In addition, a comprehensive DLT audit would provide the organization's governing board confidence that:

- There are no operational issues with the DLT system.
    1. Identify and manage blockchain risk, which might have a significant reputational and/or financial effect.
    2. Provide management with a comprehensive view of blockchain technology that encompasses technical and non-technical aspects

You can also use the following table on EY Atlas as an example.

Table 12

Common IT risks and corresponding common ITGCs

Risks		Example Control
Risk no.	**Common IT risks**	**Common ITGCs**
Manage Change risks		
MC1	New IT application programs or changes to existing programs, including reports, configurations and interfaces, do not function as described or requested because they are not adequately tested by appropriate persons.	**MC1a:** Changes to the IT application are tested by business and (or) IT users, as appropriate, prior to the move to production.
MC2	New IT application programs or changes to the production IT application programs (including reports and interfaces) are not appropriate for the business or the IT environment.	**MC2a:** Changes that affect the IT application are approved by business management different from the requestor prior to the move to production.
MC3	Programs in production are not secured permitting developers to move unauthorized or untested changes into the production environment.	**MC3a:** The programs in the test environment, including tools to move the programs into the test environment, are accessible only by a limited number of authorized, appropriate persons who don't have development responsibilities.
MC4	Configuration changes made by IT personnel are inappropriate or unauthorized.	**MC4a:** Changes to key configurations (that should be specified in the control) are logged and the log reviewed by knowledgeable persons who cannot change the configurations being monitored.
MC5	Multiple instances of the same IT application that should be identical are not the same.	**MC5a:** Changes are pushed to all instances at the same time.
Manage Access risks		
MA1	Users of the IT environment aren't the intended users due to inadequate authentication and security settings.	**MA1a:** Password settings are appropriate for the environment and level of risk.
MA2	Access rights risks: '- Access granted to the IT environment (IT and Business) does not match the access approved - Access termination requests are not fulfilled timely - Access rights to the IT environment (IT and Business) do not remain appropriate over time.	**MA2a:** New or additional access rights are approved by an appropriate management person in advance of the access being granted. **MA2b**: Access rights no longer needed by users who are leaving the entity's employ or who have changed job responsibilities are ended timely based on notification from HR or the user's supervisor or manager.
MA3	Users of the IT environment (IT and business) are not appropriate.	**MA3a:** Access rights are verified periodically by appropriate management personnel. **MA3b:** Privileged (user) access is limited to appropriate individuals and systems.
MA4	The access of IT users of the IT environment creates segregation of duties concerns.	**MA4a:** Logs of the activities of persons with access that creates segregation of duties concerns are reviewed by knowledgeable persons who do not have such access, or the changes are matched to approvals.
MA5	Access to functions within the IT application is combined into roles. The access rights within the roles contain segregation of duties issues that could cause a material misstatement of the financial statements.	**MA5a:** There is a defined process to change the access rights within the roles that includes approval by appropriate business management.

MA6	Direct data changes are made without authorization. (Of higher risk when there is routine use of direct data changes in the processing of transactions relevant to the financial statements.)	**MA6a:** Direct data changes follow a process that includes approval by an appropriate person other than the requester and pre-implementation testing or post-implementation verification of the accuracy of the change.
Manage IT Operations risks		
MIO1	Hardware or software issues result in loss of data or the ability to accurately process that data.	**MO1a:** Programs and data are written to backup media at daily and stored in a physical location separate from the production equipment.
MIO2	Issues with programs that cannot process to completion are not addressed or are addressed inappropriately.	**MO2a:** IT personnel monitor the execution of the job schedule and take actions appropriate to the issues that arise.

Note. From *EY Atlas* Copyright 2022 by Ernst & Young Europe LLP. Reprinted with permission.

Respondent 3: Employee at Corda Network of R3[1]

I: Thank you for your time. This interview is part of my thesis, which is about the auditability of the consortium blockchain. Blockchain has become hype since the introduction of bitcoin, and many start-ups and big organizations have joined the trend. Many of these organizations need to be audited, but everybody has their way of doing it, so there is a need for a standard. I know that ISO is working on their series called ISO/TC 307 Blockchain and distributed ledger technologies, which is expected to release around the end of 2022 and begin in 2023. I focus more on 'audit standards' for consortium blockchain. I will interview three types of consortium blockchain: Dual-Focused, which are you, Technology-Focused like Hyperledger, and Business-Focused, like B3i. A core part of this research revolves also around the governance of consortium blockchain. This interview will take approximately 30 minutes.

I: Could you give a brief history of your consortium and what the motives were to develop it?

R3: It all began with the concept of a distributed network of linked nodes that could be used to handle any agreement between any parties. Our objective enabled parties to assert, "I am certain that what I see matches what you see." The critical aspect was that these nodes were linked to a worldwide network where parties were aware of their trade partners their identities. As a result, in December 2018, our team established a not-for-profit organization located in the Netherlands with the mission of governing the Corda Network, which R3 founded. We launched in January 2019 and have been steadily growing since then.

I: What is Corda Network?

R3: Corda Network is a network of 'nodes' or identities that allows fast, safe, and private transactions using Corda software. As it currently stands, the network is geared toward commercial usage, and we see a wide variety of sectors joining via pre-formed business networks or groupings of legal organizations with whom they want to deal. The network has features like an identity issuance service in which membership is necessary, a network map, and at least one

[1] It is a coincidence that consortium provider R3 is also respondent number 3.

notary cluster responsible for certifying transactions across the chain. Moreover, with Corda, any digital asset may be exchanged, and any of type of tokens can be created using Corda's top-of-the-shelf software. For example, smart contract and smart legal contract capabilities and an inextricable link between contractual code and legal language ensure that settlements are carried out legally in Corda. It is possible to make automated contracting easier with the help of permissioned blockchain technologies. The parties can automate their different responsibilities after establishing a contractual connection with one another. Validation of data and the usage of tokens make this a significant step forth for businesses. This establishes trust between two different parties where typically, an intermediary is commonly used by the two parties who do not already know or trust one other to establish a contractual agreement. For example, Amazon serves as the intermediary between retailers and consumers. When customers want to purchase anything from a seller they don't know; they have to agree to Amazon's terms of use. No third-party intermediaries are required when utilizing a permissioned blockchain system to support contract generation.

I: What is the difference between smart contracts and smart legal contracts?

R3: In the technical sense, smart contracts refer to computer algorithms that automate tasks. In a smart contract, an input is followed by an action that results in an output. So, for example, when you enter numbers into a Spreadsheet and hit the sort function, the numbers are sorted in ascending or descending order, and the result is a sorted column. Whereas, a smart legal contract is a smart contract that has progressed to the point where it is considered a legally final and binding agreement.

I: What are the requirements to join the network?

R3: In order to join the network, the entity must first construct a node and then receive a Participation Certificate that grants their node permission to the network. After obtaining a Corda Network Participant Certificate, a legal entity becomes a Corda Network Participant and begins using the Corda Network Node. Corda Network Participants are classified into 'participants' and 'sponsored participants.' Participants have legal contracts with R3, whereas sponsored participants are nodes who get access to the network through a participant's agreement. All Participation Certificate requests will always come via participants, resulting in sponsored participants not seeking certificates directly from R3 because they can get access through sponsored participants who already have access to the network. Every Participant Certificate is granted to a legal entity and not a person. All Participants must submit the following information upon request as part of the network onboarding process:

- The Legal Entity's Name
- The Legal Entity's Address
- The Legal Entity's Contact Name
- The Legal Entity's Email Address
- The Legal Entity's Phone Number
- The Legal Entity's Unique Legal Entity Identifier
- Domain name of the website (Optional)

R3 has also a method for reviewing sanctions against all organizations. Organizations who do not pass R3's sanctions screening will be denied a Participation Certificate and therefore to access the network. Participants who engage in a Sponsored Participant Terms of Use agreement with R3 should not depend on R3's sanctions screening procedure for their Sponsored Participants. Sponsoring Participants are responsible for adequately guaranteeing and confirming the identification of Sponsored Participants and undertaking any due diligence and sanction checks required to ensure that all such businesses comply with the relevant Business Network's tolerance requirements. After joining the network, all Corda Network Participants must guarantee that their nodes are running unaltered Corda or Corda Enterprise software versions. However, nodes on the Corda Network may not reject communication coming from other nodes on the Corda Network that are using the routine Corda Protocol, even if they support and utilize expanded versions.

Modifications made to the open-source solution conflicting with the Corda Protocol will be declared a breach of zone policy and considered incompatible. There are two ways to join our network. You can do this directly or indirectly via a so-called business network operator. Directly is when the node of a direct participant may belong to one or many business networks. To participate in the network, they will be required to sign a Participant Terms of Use in the onboarding process with R3, pay any outstanding costs for utilizing the network, and seek a Participant Certificate themselves. Indirectly via business network operator is when a business network operator adds nodes to the network owned by a separate entity. They enter into a legal contract on account of all their nodes and are responsible for any expenses.

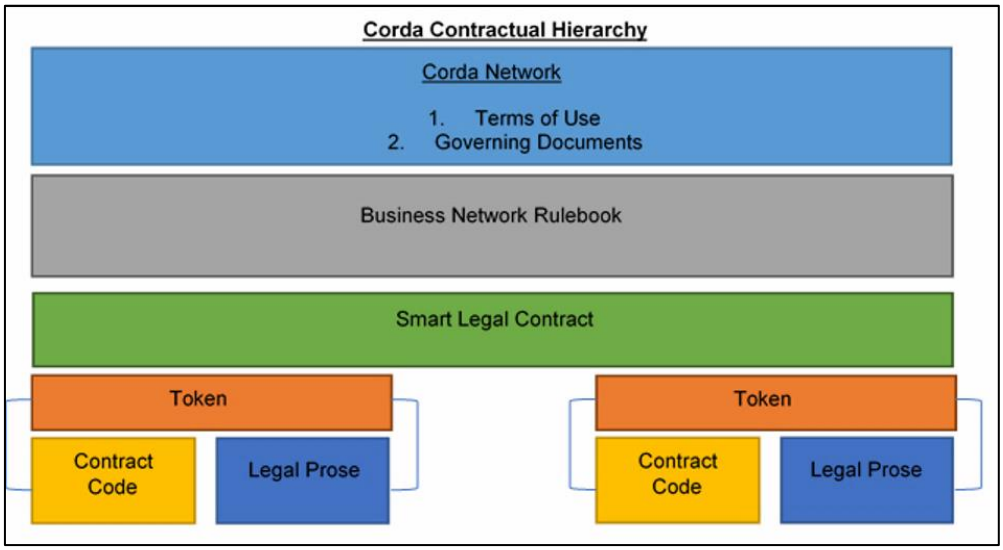
I: Is there a governance body in the network, if so how is this constructed?

R3: We have an independent Dutch Foundation called The Corda Network Foundation established to oversee the organization. A non-profit organization with no shareholders but a governing board made up of nine members who were early adopters of the network like B3i and Marco Polo and two members from the R3 network. Every member casts a vote for the board, which is then chosen in a staggered fashion by those same members. The board's goals are to keep the network safe and efficient while also allowing it to expand to its full potential. More specifically, this involves evaluating the network operator to see whether they're doing good work, deciding on price and scope, and regulations. It further consists of the network's trust root that serves as a Certificate Authority (CA) that conducts sanctions checks and provides identity certificates to nodes to join; the network's nodes are listed on a map, and the Network Operator or participants themselves can execute the consensus mechanism for nodes to interact over it. This infrastructure is supported by all nodes, allowing for frictionless transactions between any node in the network. It's being used by many legal entities, from corporations to non-profit organizations, to do business. This is important because parties must agree fairly and reasonably if they want to do business over an immutable ledger that outlines the collective's common understandings and prevents conflicts with one another. That's why participants must make up the Foundation's board of directors and have the authority to vote instead of shareholders. These directors will serve three-year terms with the primary purpose of guiding the company. They are also responsible for keeping a close eye on the Network Operator to ensure that it provides

dependable and stable service and that its users are satisfied with its work. Furthermore, they make sure that a network's participation and transaction charges are determined, focusing on maintaining low costs for users, which we call pricing the network. Also, changes to network characteristics and improvements to the system are all approved and communicated with the rest of the network, and the Foundation's structure, voting procedure, standards, and any modifications to the Foundation's governance are done correctly. We created the following governance structure, which we call Corda Contractual Hierarchy (shows picture). The structure is what we call a 'self-contained governance' model. The model's goal is to guarantee that all legal issues have been resolved. As the process moves on, terms agreed to by the parties interact to ensure that they have signed legally binding contracts and are aware of the procedures for resolving disputes in the case of a problem.

Figure 22

Corda Contractual Hierarchy



Note. From screenshot during interview respondent 3.

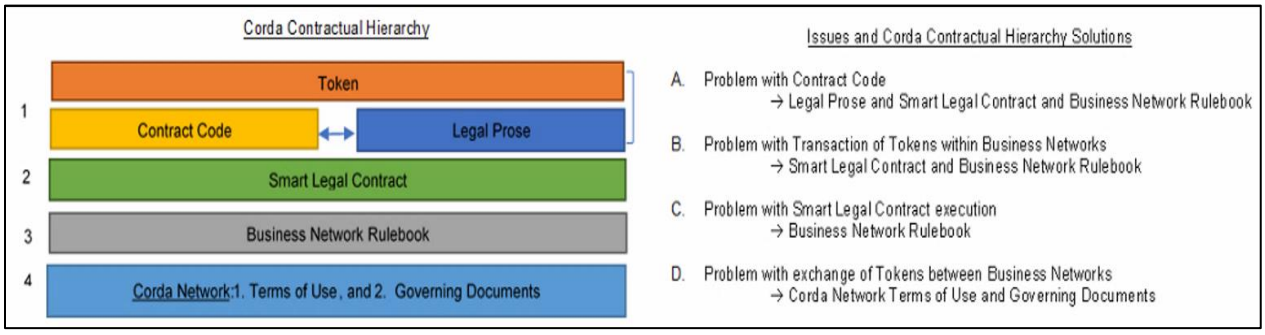
I: What is a 'self-contained governance,' and what do you mean by legal finality?

R3: 'Self-contained governance' means that there is no need for an outside expert to provide guidance on a blockchain transaction's rules or how to deal with any difficulties that may arise since these rules and procedures are included in a privately negotiated set of terms at some level of a governance structure. This is crucial because if good governance is lacking, conflicts occur which could have been prevented. Legal finality is an agreement that satisfies all of the three

legally binding criteria, is sophisticated enough to capture all relevant terms, and contains clearly defined mechanisms for settling conflicts. Finality is provided by expressly written contracts, which meet all of the legal requirements for a legally created contract and for private means to resolve disputes. In the physical world, a signed agreement might be enough to make a legal deal most of the time. But, in the digital space, this is different, especially when it comes to blockchain. This difference is in how blockchain systems and apps are set up. The hierarchy should be laid out to have a comprehensive picture of how a blockchain transaction should handle various problems. The following figure illustrates how the order may be used to deal with potential problems (shows figure). As can be seen, a different hierarchy is at work in this instance. From this viewpoint, it becomes evident that each component of the network must consider specific concerns.

Figure 23

Corda Contractual Hierarchy



Note. From screenshot during interview respondent 3.

I: When do you see governance being successfully implemented?

R3: To determine whether blockchain governance is successful, we should look at its results. For example, the stability, size, and interaction of the users with the network and how key stakeholders are involved in this process.

I: What would you consider crucial elements for drafting successful governance?

R3: A adequate governance structure should provide intellectual property ownership and license. It should show how to generate and spend money to support the platform initiative. Moreover, it should focus on selecting the correct entity, identifying stakeholder classifications,

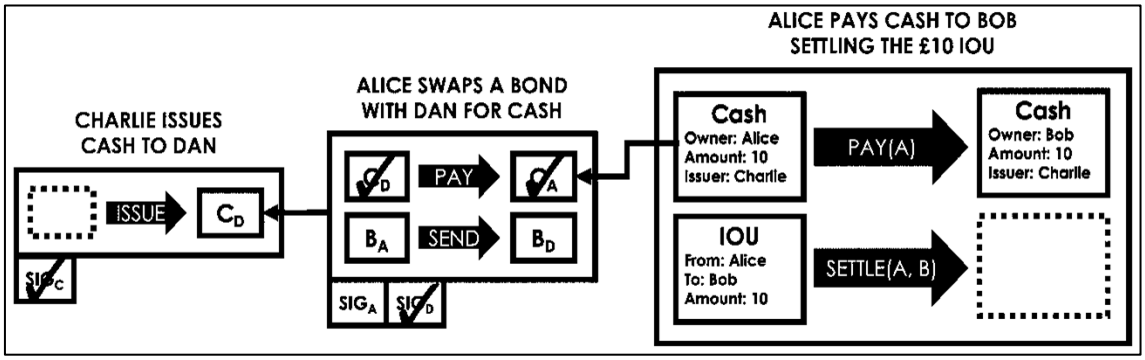
representational design, and voting privileges reserved for issues of importance. On-chain governance like DAOs (decentralized autonomous organizations) are new and have many risks involved, such as mistakes in smart contracts. For this matter, most consortium blockchains should also take an off-chain approach that is more traditional governance by organizations. Criteria for choosing the right entity could be the geographical area of the founding members or area jurisdiction. For example, if a consortium of European businesses decides to form a governing body, it is logically and likely to settle in Europe instead of Asia. Another factor of successful governance is that all stakeholders should be recognized, and decision-making power should be determined. For example, lots of networks have a variety of nodes like enterprises, service providers, academia, non-profits, and platform users. The next step is for the organizers to determine how the various stakeholder groups will be represented inside the network and how the board of this network will be organized. Many of the board's most critical issues revolve around the size and composition of its members, how it is elected or appointed, the qualified majority required for a business to be conducted, and the percentage of votes needed to approve a decision. It might be challenging to run a board if it becomes too big. The board, on the contrary, must include representation from the blockchain consortium and its most important stakeholders. Member's periods of service on the board will typically be the same as those of the board members. If the board is large enough, and if there are enough stakeholders to give Board decisions credibility, the majority will be determined by the size of the board. Additionally, how many votes each board member casts will be influenced by the structure of the board and the necessity for legality for such choices. Decisions often need a majority vote of the board's members to modify the board's composition, allocate seats among membership classes, and pass a bill. Executives are nominated by the board and are in charge of the consortium's daily operations, and the board must determine which officers are necessary. By restricting the number of Board members from a single organization or set of associated companies, many consortia guarantee that a single entity does not have excessive influence over the consortium. Finally, The board members may insist on further approval for choices like the approval of the category of members, even if board approval is often utilized for regular project decisions.

I: What type of consensus mechanism is the network application using (e.g. PoW, PoS, etc.) ?

R3: [Shows webpage] Unlike the others, Corda is unique its consensus mechanism. Before a transaction can be recorded in the ledger, it must be unanimously agreed that it is legitimate by establishing agreement. This is done by proving that a transaction has validity and uniqueness, which we call validity consensus and uniqueness consensus. Validity is proved via checking every input provided by the back-end transaction if the contracts in both the input and output states have agreed to the transaction and if the transaction has been completed with all the necessary signatures. The proposed transactions by the node, such as those that include the transfer of Treasury securities, are only legitimate by meeting the conditions if the central bank issued the treasury securities of a legal issuance process and that the security is valid in each and every future transfer of ownership. This is how the walking the chain were to look for this transaction [screenshot image from the web page].

Figure 24

Transaction example 1



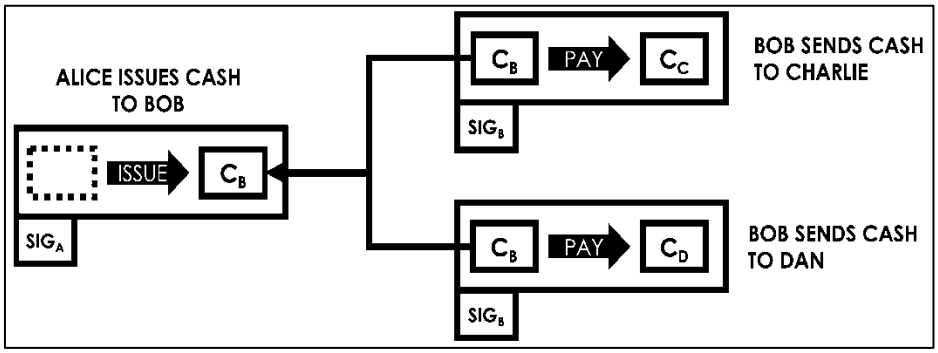
Note. From screenshot during interview respondent 3.

A node may be unable to validate a proposed transaction if it does not have access to all previous transactions in the transaction chain. If this is the case, they may request that the missing transactions be requested from the transaction proposer. The proposer of the transaction always has access to the whole transaction chain to check the input of a transaction. However, Uniqueness consensus is when a notary checks that a node has not used the same input for multiple transactions. So to give you an example [screenshot image from the web page], if Alice holds US$10.000 in her bank account, she can create two transaction proposals. The first transaction would be transferring the US$10.000 from her bank account to Bob's bank account in exchange for €9500. The second proposal would be her transferring the US$10.000 to Charlie's bank account in exchange for £8100. Both transactions will achieve validity consensus. However,

in this case, Alice would have managed to double-spend her US$ to get double the amount of euros and British pounds back, which should not have been possible. A legitimate transaction proposal can avoid this by being unique. The condition for uniqueness consensus is that no inputs to a proposed transaction have previously been used in another transaction. Double spending occurs when the notary flags an agreement as invalid because one or more of the inputs has previously been used in other transactions.

Figure 25

Transaction example 2



Note. From screenshot during interview respondent 3.

I: How do you audit the network? Is there a specific audit entity responsible for this, for example?

R3: We have all of the big four companies or actually divisions of them in our network: Deloitte Blockchain, Ernst & Young Blockchain, KPMG International Cooperative, and PwC. But they aren't there necessarily to audit nodes or the network, but more to gain from the network knowledge and then provide their services to their customers. As for auditing the network, our Corda DLT solution provides traceability of the records on the blockchain. It provides transparency to the network where each node can audit the chain for themselves.

I: In order words, there is no central entity responsible for auditing the network in general viewing it from an off-chain perspective?

R3: No not necessarily.

I: That were all the questions, thank you very much for your time and input.

R3: You’re welcome, if you have any further questions I can help you with, feel free to contact me through mail.

Respondent 4: Employee at Hyperledger Foundation

I: Thank you for your time. This interview is part of my thesis, which is about the auditability of the consortium blockchain. Blockchain has become hype since the introduction of bitcoin, and many start-ups and big organizations have joined the trend. Many of these organizations need to be audited, but everybody has their way of doing it, so there is a need for a standard. I know that ISO is working on their series called ISO/TC 307 Blockchain and distributed ledger technologies, which is expected to release around the end of 2022 and begin in 2023. I focus more on 'audit standards' for consortium blockchain. I will interview three types of consortium blockchain: Dual-Focused (R3), Technology-Focused, which are you, and Business-Focused, like TradeLens. A core part of this research also revolves around the governance of consortium blockchain. This interview will take approximately 30 minutes.

I: Could you give a brief history of your consortium and its motives for developing it?

R4: Hyperledger was launched on 9th February 2016 in San Francisco, California. It was founded to advance blockchain technology and to make it mainstream. It was established by The Linux Foundation, which had 30 founding members at the point. Among the 30 original members were well-known companies such as SWIFT, R3, and IBM.

I: What is Hyperledger?

R4: Hyperledger is a free and open-source distributed ledger technology developed by the Linux Foundation. We are open source, which means that all of our code is written by volunteer developers from across the globe and is completely free. As a result, anybody may use it and do anything they choose. In that regard, we vary somewhat from R3 or B3i. We are often referred to as an IBM blockchain or a private permissioned blockchain, and most of our installations are private. In other words, our technology is used to establish private permissioned blockchains by businesses. We have a variety of various blockchains, including Hyperledger Fabric. This is the most often used one in banking, supply chains, and healthcare, to name a few. If you look at Forbes 500, they publish an annual list of the 500 largest firms with combined revenue of at least $1 billion, half of which was ours last year. However, our market share decreased this year due to

a large number of businesses joining Enterprise Ethereum. We are an open-source organization with five different Hyperledger blockchain projects at the moment: Indy, Iroha, Sawtooth, Besu, and Fabric. Iroha and Sawtooth are both multifunctional blockchains, but a significant portion of both, particularly Iroha, is utilized in central bank experimentation with digital currencies. We have these initial retail banking services, such as currency in Cambodia and project banking in Nigeria, Iowa, and Thailand, and there are also experiments underway in the EU, such as with the ECB and the Bank of Norway. CBDCs (central bank digital currency) have the greatest prospects, in my opinion, in underdeveloped nations. Whereas if you look at developed countries like the Netherlands or Denmark, you will see that they already have similar mobile payment systems in place. In such a situation, there is little to contribute.

I: To get a clear picture. It is still not clear if consortium blockchains like Hyperledger are consortium blockchain providers, or are they being part of the network they established themselves?

R4: I understand the confusion. It was also even confusing for me because often, people think that we are IBM or at least connected with IBM and that we are selling our solution. However, we are not selling anything. We are a non-profit organization and open source, We have volunteer developers worldwide, and we provide a forum where these people can join and then they can improve on the code available on GitHub. Our network also consists of member organizations that are providers of solutions. So we have like big ones like IBM or Accenture, but we also have smaller ones like Group C and Intellect View. We point you to these people, and they are the ones that are solution providers, and that would implement Hyperledger Fabric in your particular company. Even though we are one of the biggest enterprise blockchains, our team consists of around 11 people. I am responsible for Europe. Around five colleagues are in the US. Others are in the Asia office in Hong Kong, and that's it. However, we have like hundreds of thousands of developers who are volunteers. We don't even know who they are because everybody can take the code, improve it and contribute it back to us. So our team is divided in a sense, we have community architects, and these are the more technical people supporting these developers. We have a Discord Channel with different forums, and then people can come there and talk about the problem they're facing. Then we have an ecosystem team on which I'm also on,

and we are talking with our members and our people who are and people thinking about implementing the solutions so we can point them in the right direction. Besides, these members who are implementing with you are also hosting many so-called special interest groups. These volunteer groups consist of professionals from the industries like supply chain, finance, capital markets, health care, telecommunications, etc. We're providing a forum where these people can join and have the weekly calls.

I: What are the requirements to join the network?

R4: To become a member of the Hyperledger Foundation, all Premier and General Members must be current corporate members of The Linux Foundation. Anyone, regardless of organization membership, is welcome to contribute to the Hyperledger Foundation's technical codebase. The Hyperledger Foundation Charter, as modified from time to time by the Governing Board with the Linux Foundation's approval, applies to all Hyperledger Foundation members, including Associate Members. Moreover, every member of the Linux Foundation's Board of Directors and the Hyperledger Foundation must follow the policies implemented from time to time by the Linux Foundation's Board of Directors and the Hyperledger Foundation. Furthermore, non-profits, open-source initiatives, and governmental entities cannot become Associate Members of the Hyperledger Foundation unless authorized by the Governing Board. Members of an Associate Member get no advantages or rights as a result of their membership in the Hyperledger Foundation, except for the TSC, which the TSC members choose, the Governing Board, Marketing Committee, and any other committees formed by the Governing Board may be represented by a Premier Member representative. One representative for every 10 General Members may be elected to the Governing Board each year, up to a maximum of two representatives, provided that at least one General Member representative is always present, regardless of the number of General Members. The Governing Board will determine how the election is held. Premier Members, General Members, and Associate Members are eligible to attend general meetings, projects, events, and other similar activities and declare themselves to be Hyperledger Foundation members.

I: You mentioned earlier that there is a governance board. How is the governance structured within the network, and what are their responsibilities?

R4: The governance structure consists of three components of governance: the Governance Board, the Technical Steering Committee, and the Marketing Committee.
The 'Governance Board' consists of 21 Premier Members, with one representative nominated by each Premier Member, elected General Member members, and a Chair elected by the Technical Steering Committee. The Governing Board is responsible for approving budgets governing the use of Hyperledger Foundation collected from all sources of income; appointing a Chair of the Hyperledger Foundation to supervise at Governing Board meetings, approve expenditures, and oversee any day-to-day activities; supervising the commercial and marketing operations of the Foundation; and adopting and upholding the Hyperledger Foundation's rules and regulations, such as its Code of Conduct, trademark policy, co-branding policy, and co-development

The 'Technical Steering Committee' comprises fifteen Contributors or Maintainers elected by Active Contributors who have a weekly meeting on Thursday which can be checked in our community calendar because it's open to everybody. Contributors provide code, documentation, and other technical items to the codebase, wiki, and different Hyperledger outputs. On the other hand, Maintainers are elevated Contributors who may accept change requests and upload code and updates directly to a project's archive. Additionally, anybody can join the Hyperledger Foundation as a Contributor or Maintainer. In addition, The TSC is responsible for choosing a TSC (Technical Steering Committee) Chair, who is also a voting member of the Governing Board and must act as a liaison between the Governing Board and the Hyperledger Foundation's technical leadership. Lastly, the TSC is responsible for: - Hyperledger Foundation's technical direction; - Approving project proposals under the TSC's approved project lifecycle document; - establishing cross-project working groups to address technical difficulties and opportunities; - exchanging information with other organizations about relevant technological issues; - representing other standards groups by nominating representatives; and - coordinating with the Hyperledger Foundation's Advisory Board.

The 'Marketing Committee' comprises one voting representative from each Premier Member, one or more non-voting Maintainers nominated by the TSC, and one or more non-voting representatives. There are some rules to becoming a maintainer, and one of them is the prerequisite of being a contributor to the community for some time. Last but not least, the Marketing Committee is responsible for the formulation, creation, and execution of the Governing Board's marketing strategy.

I: That's quite interesting because yesterday a call with R3. R3 had a different approach. They created a separate foundation based in the Netherlands responsible for governing the network.

R4: Indeed, Corda was created by R3, a banking consortium. So at its core, R3 started growing out of different because a consortium of companies began it. When I did my Ph.D. in 2017-18, the consortium topic started to take off. Then people try to categorize it nicely into the consortium classes business, technology, or dual-focused. Afterward, everything got a little bit mixed up and complicated. So this taxonomy is not developed at all. For example, it is normal to classify everything in biology. You had Darwin, for instance, who was like categorizing every species. But that's nature; however, blockchain is something that is not fixed at all. Especially if you're looking from the business side, the structure will bend into it wherever the money goes. And that is the problem and why it takes so long also for these standards to be developed. Because it's not driven by some natural law set in stone, we can do it and neatly draw the line between one or the other. It because it's not fixed, and it's very flexible, and therefore classification is tough to do. That could be why there is no central standard because it's changing. R3 is also different because it is a consortium of banks, and they don't like to share data with competitors and therefore need to have some privacy. That is how it started this enterprise part. I believe that they started from the mindset of the banks, which is a logical choice because data privacy is very important. However, we are seeing more shift towards having a private channel on a public blockchain. EY was one of the pioneers of that. I believe it was called the Nightfall protocol, which meant that there was a private channel on the public blockchain or public Ethereum. So it was basically like a VPN, a virtual private network on a public Internet. I think we're seeing more of this shift right towards the sort of hybrid network having a private channel on a public network.

I: Do you think that these classifications are correct? They call Hyperledger a Technology-Focused consortium and TradeLens a Business-Focused one or is it still something like, as you previously mentioned, that those organizations can throw them away because it's not relevant anymore?

R3: No. Don't get me wrong. I don't think this categorization is useless. I think it's always good to get some order into things, and I would say that TradeLens is a Business-Focused consortium. But again, if you're thinking about, for example, Hyperledger, it is not so fixed as always thought. And especially when we're talking about the business. The business part of the research is driven by what's happening out there. So you can try to sort things and put them in nice boxes. Then I think it is good because you need to have some base you can build on. But at the end of the day, the business will drive the change. So if you have a fixed box, things can get tricky down the road in a couple of years.

I: What type of consensus mechanism is the network application using (e.g. PoW, PoS, etc.) ?

R4: Each of our DLT applications have different consensus mechanism. I have a table I can share with you.

Figure 26

Consensus Mechanism Hyperledger

Consensus Algorithm	Consensus Approach	Pros	Cons
Kafka in Hyperledger Fabric Ordering Service	Permissioned voting-based. Leader does ordering. Only in-sync replicas can be voted as leader. ("Kafka," 2017).	Provides crash fault tolerance. Finality happens in a matter of seconds.	While Kafka is crash fault tolerant, it is not Byzantine fault tolerant, which prevents the system from reaching agreement in the case of malicious or faulty nodes.
RBFT in Hyperledger Indy	Pluggable election strategy set to a permissioned, voting-based strategy by default ("Plenum," 2016). All instances do ordering, but only the requests ordered by the master instance are actually executed. (Aublin, Mokhtar & Quéma, 2013)	Provides Byzantine fault tolerance. Finality happens in a matter of seconds.	The more nodes that exist on the network, the more time it takes to reach consensus. The nodes in the network are known and must be totally connected.
Sumeragi in Hyperledger Iroha	Permissioned server reputation system.	Provides Byzantine fault tolerance. Finality happens in a matter of seconds. Scale to petabytes of data, distributed across many clusters (Struckhoff, 2016).	The more nodes that exist on the network, the more time it takes to reach consensus. The nodes in the network are known and must be totally connected.
PoET in Hyperledger Sawtooth	Pluggable election strategy set to a permissioned, lottery-based strategy by default.	Provides scalability and Byzantine fault tolerance.	Finality can be delayed due to forks that must be resolved.

Note. From screenshot during interview respondent 4.

I: How do you audit the network? Is there an audit entity responsible for this, for example?

R4: No, we don't. We don't currently. Again, it will depend on the implementation as a Hyperledger. We don't provide any audits like a company. We only offer our open-source code. Now, I was just in Paris at a conference last week, and there were a couple of people came to us and said we are a blockchain audit company. And I am sure you heard about a couple of them

already, like ChainSecurity and Paladin. So when people implement it, they can create what they want, and they can either hire one of these audit companies or set it up so that it can be audited. But it's always use case dependent.

I: But for Hyperledger specifically, is there no audit firm that audits? If not, how do you assure members who want to participate?

R4: That's the thing, we don't have clients. We are solely a non-profit organization. We don't work like that. Right. The only thing we have is that we get funded through memberships, which are companies that are joining. What we do for our members is more or less sort of connecting them.

I: So Hyperledger furthermore no responsibility if there are some risks involved, for example?

R4: No, because we are not implementing the code, we are not selling it; we are just offering our code. We are an open-source company trying to improve the code and give the code out to like whoever wants to use it. That is why we do not do any assurance because we are not selling the solution to our members. I also thought previously that this was the case when I joined initially. Hyperledger Fabric, Corda, and Enterprise Ethereum are the most used enterprise blockchains. And then I also thought it was a company that sells it, but we are not. We are a part of the Linux Foundation, and we are not selling it. IBM, however, does. IBM contributed a lot to fabric and but they are the ones that will be selling you the solution. Our connection with IBM is that IBM contributed much code to Hyperledger Fabric, and that's why we are often confused with IBM. People think that we're IBM or like its subsidiary, and then we're just selling. IBM takes the source code, reuses it, and develops their blockchain called IBM blockchain. Walmart, for example, has food traceability. These are all built on IBM blockchain and not Hyperledger. It's based on Hyperledger fabric, but it's not Hyperledger. Also, like from the academic part of the Hyperledger, I'll be happy to share with you, you know, because I was writing a bit of governance myself, especially about this consortium governance. And then I was referring to it, and it's often heard as a sort of like an on-chain and off-chain governance. So on-chain is whatever can be programmed into the blockchain itself. You have these programmable rules, and

then you make them follow. You often hear that blockchain is immutable, but they're talking about bitcoin's blockchain, not really about enterprise blockchain, where you can have two or three nodes. Whereas then, and I think that's what you're also looking at, is often called off-chain governance. And these are all of how these rule sets are defined. We're talking now about some supervisory board or, like the audit nodes there, how these rules are created and developed outside the blockchain.

R4: You can say that the blockchain says it's in Burkina Faso right now. But is it really there? You still have to employ some more traditional management controls there. It's often referred to as an "Oracle problem" or a "gateway problem', meaning that you still have to ensure that the container is, in fact, in Burkina Faso and not in Nairobi, Kenya. Just because blockchain says it is there, it doesn't have to mean it is also physically. That is different from Bitcoin and other cryptocurrencies because they only exist within the system and are not connected to physical value.

I: Thank you very much for your time and input.

R4: You're welcome! Please feel free to reach out if you need further information. Because Hyperledger is a huge ecosystem, I can point you in the required direction and recommend some articles about Hyperledger.

Respondent 5: Employee at B3i

I: Thank you for your time. This interview is part of my thesis, which is about the auditability of the consortium blockchain. Blockchain has become a hype since the introduction of bitcoin, and many start-ups and big organizations have joined the trend. Many of these organizations need to be audited, but everybody has their way of doing it, there is a need for a standard. I know that ISO is working on their series called ISO/TC 307 Blockchain and distributed ledger technologies, which is expected to release around the end of 2022 and begin in 2023. I focus more on 'audit standards' for consortium blockchain. I interview three types of consortium blockchains: Dual-Focused like R3, Technology-Focused like Hyperledger, and Business-Focused, which are you. A core part of this research also revolves around the governance of consortium blockchain. This interview will take approximately 30 minutes.

I: Could you give a brief history of your consortium and its motives for developing it?

R5: I will just quickly show a screen. I won't go through this in detail. I got two slides on the history of B3i. We were founded initially as a consortium, and it was born out of a project that we had with some of our shareholders, and we focused on a reinsurance use case. We started with a reinsurance use case where many of our shareholders came together initially as a project. And from that one use case, we had proved some of the benefits. We did what we call a hackathon, where several participants were invited to play the role of the various parties that would be part of the reinsurance network. And it proved out the business benefits that we anticipated. On the back of that initial proof of concept, we became operational as a for-profit entity in 2019 called B3i Services AG, owned by 21 shareholders. There are big names you probably would recognize from the global reinsurance and insurance marketplace from five different continents.

I: What is B3i network?

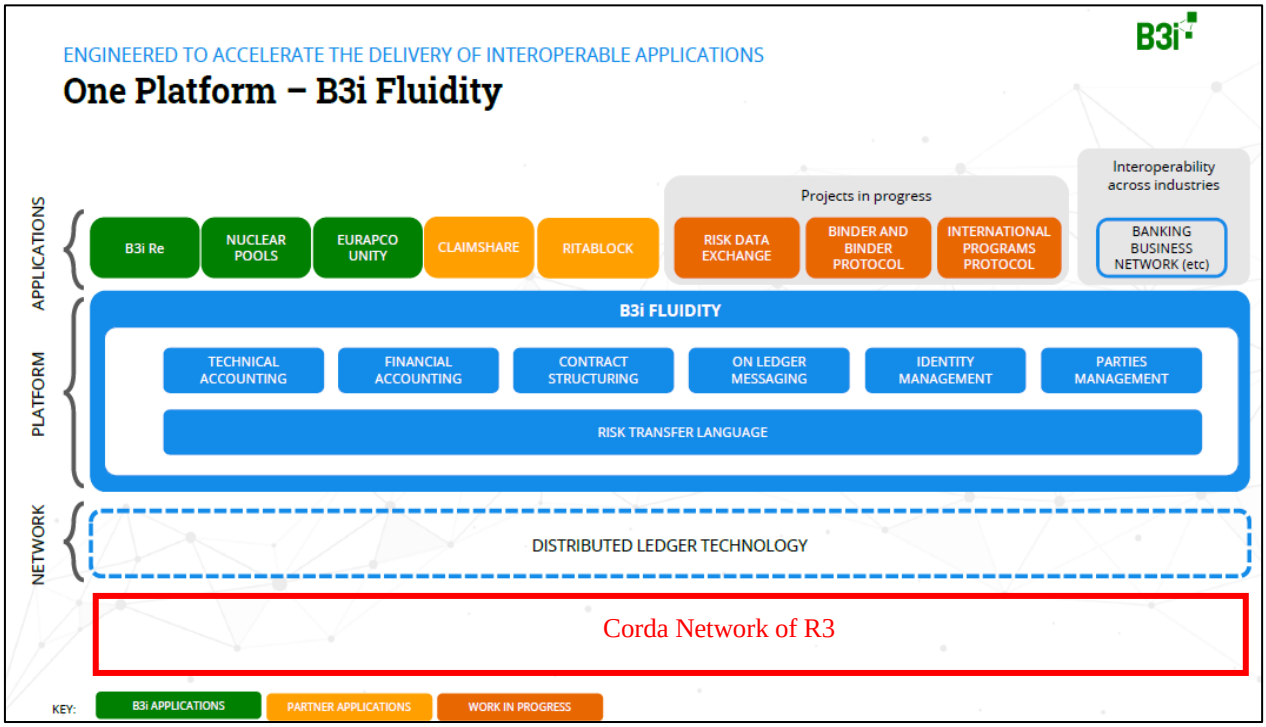
R5: B3i is a network consisting of our shareholders, which we've developed three core parts of our product and service proposition. One of the network parts is a segregated network within the underlying called Corda network. Corda is broader than the B3i network. It's like encompasses all aspects of financial services. You've got banks, insurance companies, and other financial services

providers at B3i. We've got a sub-network within their network that focuses specifically on insurance companies, brokers, and reinsurers. It's called the B3i Business Network. We've developed a platform because we recognize that some insurance-specific functionality is needed to support our blockchain-based applications. And then on top of the middle section, the platform, we have the developed applications on top. The concept can be seen as you had gone to the App Store, which is the platform, and then you downloading the relevant application within the App Store. The middle part is what we call fluidity. These are our insurance-specific components. We've built this risk transfer language that we're all talking the same insurance-based language. We've got various what we call reusable components. The concept here is that we don't want to build everything from scratch whenever we build new applications on top.

I: This build on top of the R3 platform?

Figure 27

B3i Fluidity Platform



Note. From screenshot during interview respondent 5.

R5: Exactly, R3 would be like underneath here at the very bottom. And then, on the top, you've got each application, and each application is relevant to each use case. Many of our use cases focus on the PMC and commercial insurance types, but later on, we could digress into life,

health, and other insurance use cases. B3i Re was our first lighthouse product. We built this one ourselves because this was the use case that was born out of a project with our shareholders, and it was like a lighthouse product in terms of what we wanted to use this application to show the capability of the underlying infrastructure, which is very difficult to understand and imagine without the ability to see something or log in and have a look yourself, with this reinsurance use case. There's typically a student, which is the company that's taken on a portfolio of risk, and they recognize that they've done their internal risk management and they've got too much risk, and they want to share some of that risk with the rest of the market. The student would reach out to the broker. And let's say, in simple terms, it's a 100 million portfolio of risk for natural catastrophes in the property and casualty space. They'd reach out to the broker and say, we want to share some of this $100 million worth of risk. Can you go and place the risk with the reinsurance market? The reinsurance of the broker in the middle then would help the seed. Also, in terms of structure in what that portfolio would look like, what does the coverage include the geographical scope, the perils covered, etc. They then would be reaching out to several reinsurers. And the reinsurers could be anything from one to 20 to 30 to multiple reinsurers to share some of this big risk. And this sort of end-to-end process is really exactly what happens in the reinsurance administration space. There's a period of a quote where the broker asks the reinsurer to provide a quotation for their share of the risk. There's what we call a firm determines whether to confirm their share of the risk and then sign to confirm their share of the risk legally. And then we get into all the payments because in return for taking a share of the risk, a premium is due and commission is due for the brokers. And then, if a claim is made, all the participants need to pay their share of the claim. And then, at the end of the contract period, the contract is renewed. The reason this is quite a busy diagram is that there's a lot of back and forth interaction with emails, attachments, PDFs, Excel spreadsheets, and phone calls, and a lot of that leads to big administration problems with reconciliation because people are sharing different versions of the Excel documents or different versions of the PDF that calls causes a lot of administration and time delays. At B3i, we've built this blockchain-based reinsurance application. The part that I was going to show you is in terms of the audit trail; this is the part that I was thinking might be of interest, which is where you can go into the contract. Within this is the blockchain-based application, you've got the risk details and the preliminary, which is basically where we start to structure the treaty, and it will go into layers and sections so that many risks will be broken down

into various layers and sections. There's going to be some contract wording to describe the territorial scope of the coverage scope, as I said. There will be some supporting documents like attachments, Excel attachments, etc. Then the participants will go into that. With all these online interactions, you can click into the audit trail. Each party needs to know exactly what's changed when changing the contract. And the audit trail screen provides a summary of all the changes between the current and the previous version, and a new entry is created every time the contract is shared, allowing the user to trace all the changes since the beginning of the negotiation.

I: What are specifically requirements to join the network?

R5: We do the KYC to make sure that the company is who they say they are before the onboarding to that network. And to be able to access the network, you need to have what we call a node. When you log in to the blockchain application, you log in via a node. It's just a technical term for the log-in section. And customers have got a choice. They can develop the technical setup on-premise in their own IT infrastructure, or they can have B3i node as a Service (NaaS), which is where we have a subscription model where you can subscribe to our node as a service model. Once we've done our KYC (Know Your Customer) and technically set up the node as a service, companies can join the B3i network. We require a software license agreement to be signed, a copy of the business license/register, details of the authorized company representative to enable us to add users to the node, and a fee to be paid to join the network. And in the once they are a member of the business network, we've then got a legal agreement, which is all the terms and conditions and terms of being a member of the business network. We then have relevant license terms to say what the procedures are once you become a business network member.

I: What type of consensus mechanism is the network using?

R5: Because our platform is built on the Corda platform, the Corda DLT consensus mechanism apply for B3i Fluidity. In Corda transactions must achieve validity consensus and uniqueness consensus to be committed to the ledger. For details: https://docs.r3.com/en/platform/corda/4.8/open-source/key-concepts-consensus.html.

I: Who or which entity is then responsible, for auditing this?

R5: That would be the participant's companies. At the moment there would be an existing practice between the seed and the broker and the reinsurer. They would have whatever their existing practices with auditability of various different reinsurance contracts that are placed. Whereas what we've done with our application is we've basically digitized the contract.

I: I'm also very interested because this is an audit function within the application. That would that would mean that every participant or every node has the ability to do an audit for themselves. there is no not there is not some central party with responsible for auditing.

R5: Exactly, everyone is looking at the exact version of the truth. We have a step called 'Create the Treaty'. Here, we're putting in the different layers, and this is basically where you break down that one risk into various layers and sections and whatever, whatever amount of risk the reinsurer is happy to bear. They're putting in the applicable law what's contained within that portfolio, the class of business. It's property, the geographical area, the coverage. And they've built this second layer there. If I go to the top right, I can always see who's perspective we're looking at here because this demo is going between the seed and view, the broker view, and the reinsurer view. Fast forward a bit; they've now involved the broker. An external company is now looking at the exact version of the contract. What the broker is doing is they're going through the contract and making a recommendation. For example, the student might be based in Europe. The broker might be placed in Africa, for example. They might use their knowledge to recommend that they change some aspects of the contract. The brokers made some suggestions. They've shared it with the agent they've confirmed, and now they've reached out to the reinsurer. And the reinsurer is now looking again at the same version of what the seed and the broker have already looked at. They might look at the overall risk and decline it. Or We'll take some risk, but we don't want to take all of it, then they'll propose to modify whatever they're comfortable with. They might have excluded a country, a peril, or reduced the coverage amount. But then I made in their own adapted version of the contract and said, here, look, we propose to proceed with option B, and then the broker's role in the middle will be to aggregate all the different coverages and decide, you know if they can place the entire risk. And obviously, that will be done with Excel now

because they'd be, you know, manually getting all the views back from the reinsurers to make sure this 100 million risk is placed, whereas now they'll have like a digitized version. Not only have we digitized the financial information like the commissions and premiums, but all the wording has been digitized in terms of the coverage, like the countries, etc. And then, as we go through, they're submitting what they call the firm more determined. Like the final terms, and then they get ready for signing. And you just fast forward a little bit to the endorsements if you want to change something and then sign in proposals, if you'd actually negotiated off ledger and now you want to bring it on a ledger, but you'll see here there's a button that says submitted for signing. Once you've agreed on the contract, you submit it for signing. And one of the features that we've recently developed is a dual signature to support legally binding contracts. Once again, from an auditability perspective, you know, firstly, you can make sure that the person with the authorization is given access to the application, and you can set their limits to make sure that they are registered as an authorized signatory within the blockchain application. This is an old version of the application, so it's not showing you the latest feature. But let me skip to a different view. We've recently done a paper about legally binding transactions, and I think we've got a screenshot of the new functionality. We've just had a super quick look at this beginning stage, which we call the placement stage. You choose an option to say that you want to sign into steps, and then down here, you've got a pop-up box that says, Please read these contract terms carefully. You're about to enter into a legally binding transaction by clicking this box and then going back to the audit trail. This would be able to show you precisely who signed and when they've signed, and the end pulls end-to-end auditability goes in through all stages of the value chain.

I: And each of them has of course access to the application and can audit for themselves. Don’t you have the issue that the audit can be overdone like each of those notes is going to do all that for themselves. Instead of having one entity with responsibility for auditing the network.

R5: We've built this functionality based on how the insurance companies or brokers, or reinsurers want to use this functionality to satisfy their audit requirements. We are not mandating how it is used; we're just providing the information. Because it's been digitized anyway, you got this individual ID. What is unique is that you've got this one contract idea. You can see the digitized version from the beginning to the end. We even went into the technical account in the claims, the

settlement at any point throughout that end to end contract journey, you can refer back to this unique ID and refer back to all of the digital changes per user. We make an app for our demo environment. At the moment, it's showing company changes, but with our new functionality, it can show changes down to the individual underwriter or individual authorized signatory.

I: Nice to see your on-chain audit solution. I'm also very curious how the off-chain part is done. That's more of the governance aspect, which has a big role. So, for example, if one of the shareholders lost their private keys? For example, those who have access to the private key can access the application, but it's more of an off-chain aspect, where the governance part has a role in it. Is there a governance structure, and how is B3i structured?

R5: In terms of the key part you mentioned, we'd follow our IT security procedures to ensure that we would prevent any keys from being lost in the first place. We'd follow all of our protocols regarding the onboarding and the safekeeping of certificates and things like that to access the network. And then, in terms of the governance of the network, as I said, we do a quick check for the initial onboarding. We make sure that the company is who they say they are. That then enables us to do the onboarding to the business network. And in the once they are a member of the business network, we've then got a legal agreement, which is all the terms and conditions and terms of being a member, being a member of the business network. I don't know the specific terms off the top of my head. I'd need to check what's in the license terms, but we then have relevant license terms to say what the procedures are once you become a business network member.

I: To give an example, I talked with Hyperledger previously. What they did was they had a kind of structure where there was a distinction in function between the nodes. You had, for example, Premium members who have voting power, and then you had other nodes which could participate. In other words, there was a distinction among the participants. And premium members can appoint a representative to the Governing Board, the Marketing Committee, and any other committees established by the Governing Board. The Governance Board then could vote or make decisions within the network. I am interested in who is responsible within the B3I network and who has the decision right to make big decisions. Is there also a voting system?

R5: I don’t know. I need to check it with our product team. I’ll take that question away if you don’t mind. Are there any other questions you wanted to cover, or was that the main one?

I: An additional question I have is: what are B3i’s business goals, because I couldn't find that on the website?

R5: I have them in my PowerPoint sheets and will share them by mail with you. And then your last question about the voting system and the node members, I'll come back to you one after I've checked with our product team.

I: That would be nice. Thank you very much. I won't take much of your time. Would it be possible that you can share that that those sheets which you just showed and is it possible I can have some follow up questions?

R5: Yes of course.

Respondent 6: Blockchain Expert at EY (II)

I: Thank you for your time. As mentioned earlier, this interview is part of my thesis about the auditability of the consortium blockchain. Blockchain has become hype since the introduction of bitcoin, and many start-ups and big organizations have joined the trend. Since then, there have been lots of scandals, as you maybe know, like Mt Gox. Many of these organizations, therefore, need to be audited, but everybody has their way of doing it, so there is a need for a standard. I know that ISO is working on their series called ISO/TC 307 Blockchain and distributed ledger technologies, which is expected to release around the end of 2022 and in 2023. I focus more on 'audit standards' for consortium blockchain. I already interviewed three types of consortium blockchain: Business-Focused: B3i, Technology-Focused: Hyperledger, and Dual-Focused: R3. A core part of this research also revolves around the governance of consortium blockchain. I will eventually deliver a concept audit framework for consortium blockchain. I wanted to interview you to check a framework consisting of controls derived from different frameworks like COBIT and standards like ISO270001. This interview will take approximately 30 minutes.

R6: All right, interesting. It's something we spoke about during the workshop sessions during Europe West Technology Risk Conference 2022.

I: Indeed, I participated in that one. As there were some really interesting points regarding the need for standards. Can I have those slides, please?

R6: Yeah, sure. I will send it to you.

I: All right, thanks, it was this particular slide:

Figure 28

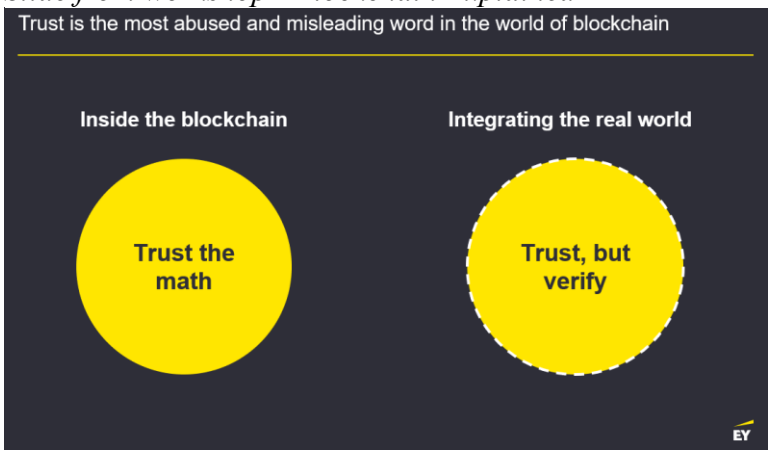
Slide from workshop "Blockchain Explained"

Note. From screenshot during interview respondent 6.

And this one:

Figure 29

Slide from workshop "Blockchain Explained"



Note. From screenshot during interview respondent 6.

But going back to the conceptual audit framework can see my screen right now. I marked the controls screen, which can be used in my case for the network governance aspect. And I marked the ones red, which aren't necessarily for my research. So I'm looking specifically at off-chain controls instead of on-chain. So I mark everything related to automation, etc., red. I'm looking more at the governance's soft and off-chain side of the governance.

R6: Okay. So when you say off-chain, it refers to the infrastructure and how the infrastructure communicates with each other. Like we're talking about the nodes?

I: Yes, indeed, the nodes of the network. I specifically also refer to what is not part of the system. The communication is, of course, done on the system, the DLT. But everything off-chain I refer to, either physical or digital (that is not on the blockchain), for example, the database of a particular node.

R6: Yeah. Understood.

I: So if we can go through all of them to check if they're correct, that would be nice.

R6: Sure, looking at the first six controls, they are clear. As for control 7, it's interesting that it's something that in the past, even five years ago, was in discussion. Right? If you have a decentralized or distributed ledger or database, how do you know that your data complies with the different regulations or policies? If you don't necessarily know where the data is located. So obviously, in a consortium, you have some grasp on where the data is located since it's the consortium that determines where the nodes will be located. So the different actors, different shareholders, stakeholders. But if you have a consortium between multiple companies, you need to make sure that all the companies comply with all the regulations that the companies need that make sense. For example, if you have a multinational that operates in Germany and then another company in the consortium that operates in the US, you must comply with both regulations. So both companies will have to have their nodes and the way they store the data compliant with both regulations. So this control definitely makes sense. As for control 8, 9, and 10, that also goes for them. This is related. So one is more technical. One is more in terms of legal. You have to ensure that if you have more than one company in the consortium, that is the whole point of a consortium. Ensure that all the people acting within that sort of internal, semi-private network are. We are aware of their collaborators and jurisdiction. Yeah. So it's all the exact answers, so those are very pertinent. And then, if I look at the red area location system, other automated means cannot operate. Yeah. I see why you put it in red. Because you're focusing off the chain, you could also have come off-chain preventive controls. But, for example, we could say that the network is not allowed to connect to nodes outside the IP address range to make sure. For example, all the network nodes are located in the approved regions. Like you could have something that is off-chain in terms of preventive control. Yeah, you could tell the nodes do not connect to any of your peer nodes if they're not within, you know, those pre-approved IP addresses to ensure that you whitelist the IP address that is in jurisdiction or regions that are not sanctioned. Like, a node from Russia pops up in the network. You say, do not connect to it. So this is an automated control that you could do. But it's okay. I see why you've scoped it out. Do you want me to go through all of them, or do you want to discuss some specifically?

I: Yes, to validate or check them all. Maybe we can go through them and say if it's or isn't correct. And if not, of course, I can put an explanation and reformulate them.

R6: Okay. So control 11 contains on-chain related elements, for example, smart contract. However, some parts of the consensus can be unchained, too. So if you want to ensure you're off-chain, you should keep it. But you should reformulate it. To take off the elements on-chain, you could say the consensus between nodes instead of the on-chain consensus mechanism.

I: All right, I will note it down.

R6: Issue because if you're talking about, I mean, it's very vague. I'm not sure because when you look at when you say assets. For example, a node is off-chain if it's physical assets. Now, it's on-chain if you talk about assets as data or the same sort of software. But then, the whole point of the blockchain is that you cannot take it out as software assets. So. To me, it could be green if you again reformulate to make sure that those terms refer to the actual physical hardware.

R6: I agree because if I look at your column A and I see transaction verification, that for me when I see transaction verification, that's on-chain, right? That's the whole point of the consensus protocol. Do you see what I mean? Yeah, the transaction is not done by the hardware. It's done by the protocol of the on-chain, in my opinion. Control 12 and 13 are reasonable; that's a good one. Not sure how you would do that, but in terms of the control itself, that's fine. You see, there's a grey zone for me. You talk about nodes that are off-chain. You talk about the data in the on-chain blockchain. You talk about how those two kinds of interact; that's great.

I: Monitor transition. In this case, it's not necessarily the distinction between physical and digital, but it's more indeed what you mentioned that what is part of the protocol that is on-chain and what's not that could also be physical or digital.

R6: Exactly. If you have an interface that automatically takes the output of a smart contract in, for example, provisions and access or creates data in the cloud. Is that off-chain or on-chain? Because it's part of the Smart Contracts concept. But technically, it's not purely data that comes from the blockchain. There's this interfacing that, to me, is still grey and could be solved in terms of vocabulary.

I: Indeed, that's a good one.

R6: Yeah. And I think you won't find a precise answer when you go to technical parts like this. So it's up to you. In your thesis, part of your introduction or part of your first paragraphs is to define how you want to treat those words, how you want to define those words, and what I would do in your case. Okay. Monitor transmission and size of the legitimate. Sure they can. Again here. We're talking about networking, but we're talking about networking in terms of package size, which is directly correlated to. How your network scales, which is directly correlated to. To your protocol of the chain, right? Because if you have a protocol like Bitcoin where you have 10 minutes between blocks, the fact that the. The replication takes a few seconds. It doesn't matter, right? Because you're not looking at speed in terms of performance. It's not a significant KPI that you have this replication that happens instantly, whereas you have a blockchain where you know. Transactions where you want. The information is nearly instant, and that's a significant KPI. So to me, that's still off-chain. But yeah, for me, it's still off-chain because it's. It would impact how you think about your size and speed. You can; you can keep it like that in green. Protect the network from access. That's have changed. I mean, there's nothing there that's on-chain. We're talking about rogue nodes. Right. And that would the way you would prevent this is very similar to how you would prevent a node from connecting from Russia, for example. You would have a whitelist of known nodes within the network. Yeah. Either a whitelist or a blacklist. It depends on how you want to treat it. You can block certain countries or specific areas. The only thing with the whitelist that I can see is that because of consensus, you're not in a purely private blockchain, so you still potentially have people that get appended to the network without contacting all the participants. And so you would have to update that whitelist all the time, you see. If you have a new company that joins that consortium, they would need to inform all the other companies that this company has entered and has added a new node or new nodes. Every time you add a node, you would have to inform everyone. So it's a bit difficult management, but this is the best way.

R6: Employs secure and preventive analytics. Okay, so that to me is a change of course, because you're not even though you're looking at the data of the chain or the protocol, you're. You're completely separated. The monitoring is not part of the blockchain. It's the first time. Hash collision. Is that a risk? In some blockchains. Do they have small enough? Hash sizes that it could

generate a collision at the probability level that's low high enough that it would be significant. To me, it's. Super easy to prevent, and it's the odds of that happening is one in a gazillion. So anyway, it would be very low. At least for using a classic quotation or classic hashing. I don't see that happening. But anyway, let's move on. All right, control 16, the Appropriateness of KYC, this is the number one issue we had when those Bitcoin and Ethereum we're using as transactions is how do we know who's behind it. As long as it's on-chain, you can trace it. But how do you link a public key and the physical person or entity behind it? That's super important.

I: This was also the one which, like, as you mentioned, it came like it was the most important part, which my interviews with the consortium blockchains which they mentioned actually.

R6: I don't think control 17 would be unchained because you cannot revoke. You cannot delete a private key. You could not revoke access to a private key of someone if somebody jotted down the private key. There's no way for you to say to the blockchain, stop accepting this private key. It's all cryptographic. The whole point is that it's anonymous. The only way to implement that is to have a second layer of authentication where the private key is never disclosed to the personnel. And that you revoke the access to that private key to the personnel. You needed that. At least from my perspective, the only way you could do this is to have this private key locked in a box like a ledger or a nano or some other solutions that exist right now. And that when a user wants to do a transaction, they never use that private key. They never see that private key. They use another ID in that black box. Sign off this transaction for me. But that black box never discloses the private key. So that whole system that I just described for me is entirely off-chain. It's a layer above.

I: Right, that would also be the only way. Right. So indeed, on the on-chain, you couldn't do that. That's not possible, as you mentioned.

R6: Well, I don't know all the blockchains in the world. So maybe there's a way to block a private key from doing transactions on the blockchain in some systems. But if it were to do that. It would take off some of the power of the blockchain itself because if you could have a validation on the blockchain of who can write or sign the transaction. Take a public key. How

could you block it and have the in quotation mark miners not? Yeah, you could, but I would still put it classified as off-chain to me. But it would be interesting if you had another discussion with the people developing those solutions. How do they manage this today? Do they use the second layer of security? Do they integrate it into their protocol directly? I mean, this is something you could ask if you have another discussion.

I: Indeed, it would be good to talk to them again.

R6: Control 18 is off-chain for sure.

R6: Control 19 is basically the 51%. This also applies to public or semi-public. From my understanding is that it's a group of organizations or people that create their private blockchain, which is no longer private because it's part of a group. So those in this group agree on their way to do it. So if you have, for example, the Microsoft blockchain for Xbox and then you have Nintendo, that comes to it, right? Well. Microsoft owns one of the two companies, by default, owns at least 50% of the nodes since the two companies own 100% of the nodes.

I: Okay. And in the case of a consortium like, for example, for that network, they have like 100+ participants. Would that be a significant amount? Would that be large enough?

R6: Yes, there would be large enough as long as those agree on that. Yeah. As long I mean, it depends on what you want to do if you want trust between the participants. That's why I believe private blockchain or small consortium blockchains will disappear and are not the future is because the whole point is that you can trust the network without trusting the other party. But if the other party is the network, then how do you trust it? So I would keep it, but it only works in, as you mentioned, a vast number of participants. I would say maybe ten or more or something like that, you see.

I: Should I put it in brackets by ten or more?

R6: Sure. That's the same thing we saw earlier in our discussion. It depends on whether that permission, that identification of the different nodes and the way the protocol communicates, the information you consider on-chain or off-chain. It's for me, that's a bit of a grey area. It's before it becomes unchanged because it's before it becomes appended to the blockchain. But that is definitely part of the blockchain protocol. If the definition of on-chain is that everything is directly linked to the data stored on the chain, then no. If you're on-chain definition is everything that is part of the protocol that allows you to put that data to be appended or stored on the chain, then yes. So it is up to you; it depends on their definition. As for control 20, that's off-chain for sure. That is the Decentralization or enforcement of consensus protocol. The one is off-chain. I mean, that's part more of a jurisdictional jurisdiction. I mean, you're not talking about automation or anything. You're talking about whether people are able or not to do some inside trading.

I: All right. That was it.

R6: Any other questions?

I: No, thanks. So I'm going to cross-check with other experts within EY. And as I mentioned earlier, I want to see I'm going to take all those points from the practice side and I'm going to check them with the theory side. And I'm also going to check it by, for example, an expert to see if the controls are correct or not. And that's interesting to see what the difference are. So maybe the other person may come to a different conclusion. So thanks for your feedback and review.

R6: So when you're done with your thesis, will it be available, or will I be able to have a copy of it because it's a very interesting topic?

I: Yeah, of course, I will definitely send a copy. Thanks for your time!

R6: You're welcome. If you have any more questions, feel free to contact me via Teams or by email.

I: I will really appreciate it; thanks again.

Respondent 7: Blockchain Expert at EY (III)

I: Thank you for your time. As mentioned earlier, this interview is part of my thesis about the auditability of the consortium blockchain. Blockchain has become hype since the introduction of bitcoin, and many start-ups and big organizations have joined the trend. Since then, there have been lots of scandals, as you maybe know, like Mt Gox. Many of these organizations, therefore, need to be audited, but everybody has their way of doing it, so there is a need for a standard. I know that ISO is working on their series called ISO/TC 307 Blockchain and distributed ledger technologies, which is expected to release around the end of 2022 and in 2023. I focus more on 'audit standards' for consortium blockchain. I already interviewed three types of consortium blockchain: Business-Focused: B3i, Technology-Focused: Hyperledger, and Dual-Focused: R3. A core part of this research also revolves around the governance of consortium blockchain. I will eventually deliver a concept audit framework for consortium blockchain. This interview will take approximately 30 minutes.

R7: Nice topic. Several years ago, I also did my master thesis on blockchain, which revolved around blockchain applications. So I am very curious to see where you are heading.

I: So, I sat down earlier with another EY colleague who is a blockchain expert to filter down some controls based on other existing audit frameworks like COBIT and standards like ISO27001. I like to cross-check this with you. Did you have the chance to look at the controls I sent you via mail?

R7: Yes, I checked it. I have some. Points that I think could be discussed. But overall, I think it makes sense. But, depending on the setup of this consortium, etc., it might need to be adjusted.

I: Yeah, I talked to three different consortiums, and they are classified into three types of consortiums. So I interviewed each type of consortium, starting with a business-focused consortium that does provide DLT technology for commercial use. Then you have like technology focus, mostly nonprofit foundations like Hyperledger, it's open-source, and then you have dual-focused who do both to commercialize software and have an open-source usage. The general conclusion of those interviews was that it is primarily the off-chain site that needs focus,

as the technology already has functionalities that prove auditors to trace back transactions and audit this, and that the off-chain in regards to governance needs the focus. So looking at the controls, what are your suggestions?

R7: So you have this control 15. It states that it should place a control on 51 percent attacks, for example. So basically, each network firm would need to ensure that their IT systems and everything is under control. As the 51%. attack depends on how many participants you have. If the participants' amount is small, this would not be easy to realize, and you would need to make some kind of mechanism. So in the case of 51% attacks, if you have five parties and three of them decided to corroborate, you probably cannot avoid it unless you have some other mechanism or an incentive. My follow-up question would be, how do you do it. I.e., how realistic would it be to implement this kind of control? So the control itself is theoretically correct but practically hard to implement.

I: That's an interesting point. The practically of the control is not in my thesis scope, but it is essential to take into consideration. But it's an interesting point because it is equally important to have a realistic and feasible control and not something impossible to implement.

R7: As for control 14, I have the following remarks. What do you mean precisely with access in this case? So just generally, what is the idea of access here? Do you mean only the parties involved in this consortium blockchain have access and/or employee user or client users of the individual firm node that can access the data? So what is the scope of the entity? Who has this off-chain database? It's about keeping today's employees, for example, who come and go out of the company. That's probably, in your case, different kinds of companies, types of companies. And they all have their own off-chain, which could be an SAP or something.

I: That's an interesting point. I guess it would be to take the firm as a node instead of each particular company user. So it's broadly the company itself. And then, indeed, maybe it's interesting to look in the individual user lever of the node, which are persons in that company, and to see who should have access and who should not. Is it that all the persons in that entity should have access or limited persons? So that is a good one.

R7: Indeed, in the end, you have several options going into this one blockchain or putting data into it. And then it could also be that the participants of this consortium are changing, that they have some new companies coming in and are not part of it or are temporarily part of it. And in that case, it's probably the same: it would need to be adjusted.

I: So, to see how well the users within that entity can be regulated, who has access, who is not. So I will take that as a note here.

R7: I mean, in the end, it's a database. What goes into this database so you can audit it? The point is, I think if you have a control over how the data comes into it. Or if there are any checks of the data when it enters. In the end, the intended and relevant information should only end up in the database, I guess, in the case of payments. That's pretty simple because you can say, okay, you need to attach a payment receipt or an invoice payment receipt. So every transaction can also be proved that it's legit. This is looking at it from an audit view. I'm not sure if you're aware of the IPE (Information produced by the entity)?

I: I heard of it, but I don't know much about it in detail or how the process works?

R7: So basically, there are five risks. Four are related to the data extraction transformation of the client data. But there's one risk about what data goes into the system. And that cannot be audited just exclusively with analytics or these things. So there, you need to manually test what goes into the system manually. So maybe just as a proposition, for example, for payments, is that you need to upload or test, it automatically checks where you also need to upload documents. Where it can verify that it's a legit transaction. But overall, I think it's a very good concept. It should probably be customized to individual cases. That's what I always think in reality; the theory is always the theory, and you need to adapt it into practice. All right, these were the points from my side. But I think the controls that you listed make sense. And I think as far as I'm concerned, you did a good job.

I: Thank you very much for your time, and I appreciated reviewing these controls.

R7: You're welcome; if you have any questions, please contact me when you finish your thesis. I would be glad to have a read into it. So if you sent me that, that would be cool?

I: Yeah, indeed. I will note it.

Respondent 8: Blockchain Expert at EY (IV)

I: Thank you for your time. As mentioned earlier, this interview is part of my thesis about the auditability of the consortium blockchain. Blockchain has become hype since the introduction of bitcoin, and many start-ups and big organizations have joined the trend. Since then, there have been lots of scandals, as you maybe know, like Mt Gox. Many of these organizations, therefore, need to be audited, but everybody has their way of doing it, so there is a need for a standard. I know that ISO is working on their series called ISO/TC 307 Blockchain and distributed ledger technologies, which is expected to release around the end of 2022 and in 2023. I focus more on 'audit standards' for consortium blockchain. I already interviewed three types of consortium blockchain: Business-Focused: B3i, Technology-Focused: Hyperledger, and Dual-Focused: R3. A core part of this research also revolves around the governance of consortium blockchain. I will eventually deliver a concept audit framework for consortium blockchain. I wanted to interview you to check a framework consisting of controls derived from different frameworks like COBIT and standards like ISO270001. This interview will take approximately 30 minutes.

R8: All right!

I: will share my screen with you and show you the concept audit framework I made. Let's see if you can see my screen. Yes. So I made the framework with some categories and columns, for example, the risks, the control objectives, the controls, and the classification. And then, from the validation point, I made three separate columns with reference to practice. So the controls I have are all derived from different existing frameworks. And also, I made a column to reference the theory, so I will analyze it and try to align it with existing academic literature. And then the final column is for the check by the expert, what I call it. So I'm going to sit with different colleagues, IT auditors, or colleagues who are experienced or experts in experience blockchain to validate all the controls. Could they possibly be used in a blockchain environment or not? So as you can see then, I have put all the different columns like this. Then I put like the topic so what the topic is about? For example, regulatory compliance is all about if, for example, all controls are related to regulatory regulation derived from different frameworks. So what I previously did, I said with different colleagues and just went through them to check. Is it possible? Do you see it? So it can be used or not. And if not, maybe give some short feedback on how to enhance it. So if we start

from the above, I made a couple of controls for the regulatory compliance I derived, especially from COBIT and ISO. Do you think they could be used in the environment of consortium blockchain, or do you think there needs some adjustment? What's your what's your opinion?

R8: The first control is about defining the scope, which is the logical first step!

I: The next one is about network effectiveness.

R8: As for the second control, do you think about the blockchain as a system or a system where you can put something in it. In order words, you consider this control if you consider the blockchain an IT system, operating system, or database. But you have to decide.

I: I haven't considered classifying it perse in that way.

R8: I would suggest classifying it.

I: All right.

R8: Control 3 is essential, as you want to have a responsible entity that takes responsibility for audit procedures or is accountable in case of conflict.

I: Yes, that was also an important point derived from my interviews with consortium blockchain providers.

R8: Controls 4 and 5 are similar and a logical step in creating agreement between participants. Otherwise, you could have a conflict of interest, for example, or disputes that could have been prevented if the policies were in place. Control 6 is, I would guess, the responsibility of the blockchain provider?

I: Yeah, but I also mean the overall participants in the network.

R8: Yeah, definitely, to proceed in, for example, updating the blockchain, it is important to have users that are also technically acquainted with the necessary knowledge on blockchain. Controls 7-9 are suitable. So in countries such as Estonia and Salvador, blockchain cryptocurrencies like Bitcoin and Ethereum were regulated. So yeah, you can compute it because, first of all, before implementing the blockchain, you have to be sure that that in that country is applicable.

I: How is that, for example, in the case of consortium? So a consortium blockchain is, you know, a partnership of different entities. But for example, you have a company located in like Brazil and another company in the USA and another company like in Europe. They have, of course, different regulations. But if they want to work together. Is there a possibility that it will not align because you have different regulations?

R8: Yeah, I know. From my point of view, it is also an applicable one.

I: But it was also too good to mention that the consortium blockchain provider interviews concluded that the problem is more on the off-chain side and not so on the on-chain because, on the on-chain, they have many functionalities in their system for traceability.

R8: Yeah, because it's very interesting because, you know, on-chain, you can see everything. You have the transparency and are sure that those transactions were made on the blockchain. In that case, let's say you and me. You have your wallet. I have my wallet. Each of us put some bitcoin in there. I want to send you like 0.5 bitcoin; not that important in the amount of the money I transfer to you. It will not necessarily be put on the blockchain. All right. At the end of the day, if you have to send me something and I have to send you something or let's say for, I don't know, one month, just at the end of that month, the balance sheet will be put on the blockchain. But not all the transactions will be traceable on the blockchain, just like the last one, the balance sheet. So, in that case, some of our transactions are not traceable if they were off-chain. Now because, for example, on the blockchain, on the off-chain where you are, that would be very like. And some transactions that are not legal or don't know related to something illegal cannot be certified or traceable. So that's the problem actually with the chain. And that's the fact that. That's the reason why we auditors have to audit the blockchain.

I: All right, let's move on to the next one.

R8: Control 10, we don't have an answer from the European Commission. We did, for example, because, you know, there is a conflict between the blockchain and the European Commission. We are on with the GDPR about the GDPR because you have two articles in the GDPR, which are articles 16 and 17. You can go up to that and Google it because the articles of GDPR say that the user has the right to cancel their data. The user has the right to modify its data. And it's not possible, as you know. The Blockchain Foundation commented from their side that the data you put in the blockchain is not necessarily personal data because you can use the hash to put your data in the blockchain. And as you know, the hash is a one-way function. So you can have the hash by having the input. Your data, but you cannot have your data back by having the hash.

I: All right, I will look those articles up.

R8: Controls 11 and 12 are good. I would suggest putting in brackets a couple of examples of standards. The control (13); protect the network from access by monetizing notes, information, and public blockchain. For example, in the off-chain, you need more private keys to make the transaction. Because, for example, we are off-chain, and we want to do that transaction between that transaction, like my bitcoins from my wallet to go to your bitcoin or your wallet. I do it just with my private key. I also need your authorization.

I: So you mean like a secondary mechanism for the access?

R8: Yeah. So you don't need to just private key just on the on-chain. But also the second private key.

I: Okay. And how would you see it? Like then, that would mean that each node in the network would have a separate key. But how would you then validate? That private key that is then off-chain?

R8: It is just that the end transaction will be put on the blockchain, for example, and not all the transactions. Just the last transaction would be validating. But the intermediary transactions are not. Let's say I have like one bitcoin. I send you like 0.5, and I will have 0.5; you have 1.5. But actually, it's not like this because you will. You will not have it until the transaction is put on the blockchain. So in the meantime, you send 0.2 to me so that I will have 0.5 plus 0.2 = 0.7, and you will have 1.5 - 0.2 = 1.3. There are systems like Lightning that requires a multi-signature address. So you need, as I said, more than one private key to sign up for transactions. So the future deposit by both parties is recorded on the balance sheet. The balance is updated, and both parties sign off on it with the private keys. At the end of the exchange or business, the final balance sheet is sent on the blockchain, but not the intimidating one. For example, I have one I have to send to you. For example, 0.5. So you will have +0.5, and I will have -0.5. Let's say the second transaction. You send me 0.2. As I only use money at the end of the month. Let's say this is our last transaction. This is the balance sheet. This balance sheet is like any cell will be uploaded, or we will be updated every time we have a transaction. The last transaction would be put on the blockchain. So, in the end, you will have on the blockchain that I sent you 0.3, but you will not have these intermediary transactions.

I: Now I understand fully, so the mean the transaction in the meanwhile those are taken into consideration only just the end transaction. The final balance sheet will move on to the blockchain. But how do those transactions work? Because the transaction isn't done on the blockchain. What kind of system is used and instead, in the meanwhile until it's then moved to the blockchain?

R8: Nodes on the Lightning Network. Download the software and create change channels between themselves and another node while users have a wallet that sends or receive payments to the network on the network.

I: Could you please send me that link in the chat?

R8: All right, here you go: https://cryptoadventure.com/understanding-on-chain-and-off-chain-blockchain-transactions/. There are also many videos on YouTube about Lightning Network, the application, and how to change.

I: Previous people I sat down with had an input for control 14, for example, and it had to do with the 51% attack. Previous blockchain expert, I sat down and commented on how feasible this control actually would be. For example, in a network that is small in numbers, for example, if you have a consortium of like four nodes?

R8: You remember my colleague when he explained the fact with the attack and all the things, for example, the blockchain of Bitcoin or Ethereum or are really secure because you have many nodes. For example, we have four nodes. It's enough to corrupt three if they would attack the blockchain.

I: So maybe I could put in the control, like, for example, from, from a minimum amount that would only be feasible from a minimum amount of participants, right?

R8: Yeah, I would use this one and say it would be feasible from a minimum number.

I: And what would be a rational number to make it feasible?

R8: I cannot say that. I would mention that as long the number is significant enough. I think it also depends on the kind of business you are in.

I: All right, the next one, that is control 15.

R8: Yeah, this one is very dangerous for money laundering. I would classify this as a critical one.

I: All right, I marked that down. And control 16?

R8: That is a logical corrective measure, as you want to withdraw access to ex-participants as soon as possible.

I: A couple of final ones, control 17, 18, and 19?

R8: Those controls are audit & monitoring related. Which is important to review periodically. They look good to me.

I: All right, that was it. Thank you for your time and for taking the time to sit with me and review the framework.

R8: You're welcome. If you need further information, questions, links, or something. Just message me.

Respondent 9: IT auditor at EY (II)

I: All right. Welcome. Thank you for your time. As I mentioned earlier, I'm doing my thesis about the auditability of consortium blockchain. And I made a conceptual audit framework for auditing consortium blockchain consisting of different controls from different frameworks. I sat down with three types of consortium blockchains to interview them, and I sat with colleagues who are experts in Blockchain from EY to review those controls and their inputs. I came up with a conceptual framework, and I wanted to sit with you because of your background in IT audit. It's essential to see if these controls are relevant and what's your view or point, or perspective on these controls, especially the structure of the framework. So I'm going to share my screen with you to see what type of controls I made. Let's see. Can you see my screen?

R9: Yes, I can see it.

I: All right. So this is the control framework I made. There are different columns. As you can see, I started, of course, from your logical perspective, what type of process it is or the topic. For example, I view some topics related to network governance. And then, of course, I start with the risk. What type of risk is there? Follow up with the control objective and, of course, the controls and what kind of control classification it is. I made use of two types, two types of control classifications, as you know, preventive and detective. There is also corrective, but I didn't put that in the scope. Then I put three separate columns. Here you have the reference to practice. So here are all the references to the standards and frameworks I used to make these controls. And what I wanted to do is make a separate column that is referenced the theory, and what I mean with the theory is the academic articles and the models that are made up about blockchain or auditing, such as network effectiveness. There is an article by or professor, as you know, Martin Smits, who has expertise on that. So I'm going to put all kinds of references from there to connect and align the practice with the theory. And the final column is the column, the check by the expert, which is the IT auditors, but also the blockchain experts within different kinds of organizations I spoke to. And what I do in the end is put the names on it. I also talked with previous colleagues about how they want it to be named. Because I understand that you want to be anonymous, if you want to be anonymous, I can just put your title like it auditor at technology

risk and then the company. But if you want to be named its full name, that's also okay. So it's up to you. How do you want to be named in the check by column experts? What is your preference?

R9: Yeah, you can put my name there if you want.

I: All right. Thanks. So we're going to go through a couple of those controls I made up. First of all, let's, for example, begin by scoping. One of the examples I made, for example, is you have, for example, the risk that the blockchain is not defined clearly for the stakeholders, and the control objective could be then to ensure that the scoping purpose is formally defined and aligned between participants. And a control could be a scoping definition. The scoping definition is documented and approved by the relevant stakeholder. Do we have any? Any input or any opinion about the controls is logical? Or do you think there could be some more improvements to the control?

R9: So I have the first two questions, if possible, about how do you define a particular area? What are they based on? So you mapped what is essential? When you audit a blockchain like this, the first step you likely take is scoping or a process?

I: So what I did is that those areas are also derived from different standards. So I took out the information. It's a combination of the standards and what I could find from the theory. So, for example, I did a literature review, and I put different kinds of articles like, for example, you have the actor-network theory, you have the smart business network models, for example, by Smits, etc. And I try to align them kind of together. So I derive those subsets or sub-areas or topics I derived from the article and the standards, and I try to align them to make it chronological and to make a logical model for scoping. So when you start, for example, most of you start the project or the networking, it was logical for me to start with scope. So those topics already existed, but I moved them up and down to make it a logical follow-up.

R9: Yeah, clear. One thing I do questions about the practice. You see a combination of preventative, detective, and corrective controls. So a detective rule would only be useful if you actually act upon it. I think that's one. One thing that's important to include as well.

I: So you mean like that you can have a control that is also preventive and corrective, is that what you mean?

R9: More like, imagine an organization does not do the first control you think of in the scoping space; scoping is not documented and approved. Are there ways that the company and detect this so only preventive control might not be sufficient in terms of risk? Because it's often the case, that organization thinks of the things and follows the framework very well, if there's execution, they miss things or forget about things. So then, it's really good to have the combination of detection and to act upon detecting mistakes or things that happen. So I think it might be an essential improvement if you mentioned the corrective controls.

I: All right, I didn't put them in scope, but I wanted to limit the number of workers you can eventually make. There is no limit to the amount of control you eventually can make up. So I just thought, okay, I'm going to limit it to a couple of important classifications and then try to limit and scope it as much as possible.

R9: Yes, I think it would make sense. But I think the combination of at least preventive and corrective is the key to a good framework. Also, detective alone doesn't get you very far. Because when you dissect an issue, for example, in a network governance area. The organization doesn't have any controls in place to act upon it.

I: Okay. I got the point that it's the corrective eventually that you will act upon it?

R9: Yes. For a network benefit, for example. Then many companies have scanned in place to detect specific intrusions, for example. But if they don't follow up, for example, such management or another type of corrective action, they detect ability, but they never fix it. I think that's why you need the combination of those types of controls because the section alone of the vulnerability like that doesn't really make a difference. You don't have a good place actually to do it.

I: And for more for the logic because we're going to review the logic of the framework's structure from the IT audit perspective. Could you give an, for example, an example for control of scoping like the first control we have here? What would be then a corrective control in this case?

R9: I would really have to think about that because this is not something I see in frameworks. The scoping, I think, is part of how you approach the audit from the other perspective. Think, okay, this client has a particular question. What can we do to help them? So then you go and identify, for example, your approach, the authenticity, and the auditors, together with the client, arrive at the scoping. So that's usually part of the process of beginning. And I haven't observed this internally. It's part of the framework and you decide together with the client. But I think blockchain has probably a different story because their issue is that the risk is that you forget certain areas. After all, the object is there. So maybe you should also include a control which state that the scoping is reviewed or updated in case of changes and, for example, reviews on a particular frequency so certain that the scope still applies.

I: So, in general, reviewing would be all things related to review and could be classified as corrective or?

R9: Reviewing. I think the more the section for this, it's unclear because you cannot always categorize them like this. But, depending on how you phrase them, they are usually persistent in their review. Something might come up, or something would change, which is quite valid anymore. Then you dissect that during this review, and then updating your definition or document would be the corrective action.

I: And a follow-up question that came to my mind is the structure of this particular framework. Is it something? From the auditor's perspective, is that something logical like the structure I have or do you think there could be some improvements in it?

R9: I have to say, I'm not very familiar with the most critical risks for blockchain because it's not my field activity per se. What's more, I use many frameworks for support. Blockchain, I think

that's a very new area. Normally you identify the most critical risks based on your control objectives and controls on those risks. That would be an approach that we also know and use.

I: Okay. So the structure is logical in the case that you have, first of all, the risk you define and then the control objective and then the controls.?

R9: Indeed, you have the order to discuss the most critical risks with management, for example, because they will know what risks this company has. And then, you would also dive into the environment of the organization and the history of the organization. Things that might affect the organization today can be external or external factors. All right. If you identify those risks, you can easily define a thing as objective. It's also a bit more complicated, but I think it's safe to say the risk identification.

I: All right. Another question I have is. It has to do with the topics like the topics I defined here. For example, I started with scoping, network effectiveness, network governance, network policies, regulatory compliance, network interoperability, access management, etc. Are these like logical topics to you that have to be discussed, or do you think there are, or so to say, these are the essential topics you would usually see and use?

R9: Yeah. I think I think maybe the network ones can be combined into one. And I think they are all separated potentially. You might see them in one primary topic called infrastructure, for example. And then it's divided into smaller ones for those regulatory ones. You think about combining like this, you have four separate controls for one or two, maybe for the network ones. You could also think of something like that where you don't have all these separate controls, but it's more the combination of controls that supports the network.

I: All right, then, that is nice. And another important question that came to my mind was, do you think it would be better to put the preventive, detective, and corrective controls per topic? So I do all the three per topic. Would that be something that would be more logical for the framework?

R9: It's a great approach, but it's not always possible to have all three. It also depends on the topic's importance. But it is possible. Also is one of those controls that fail. Then you have two other controls to remain. So then, if your preventative control fails, you can still do a good job if you detect and correct the errors. So, in case something goes wrong. I think it might be a good approach to put the corrective measures as well.

I: Okay, that's nice. And then eventually, coming to the final question would be, are there first of all, before going to the last question, you gave an example of those data sets. Do you have an example where those controls are classified in an Excel sheet that I can look into it?

R9: Yeah, sure.

I: And my final question would be, are there other things you would say that miss in this framework that would be really relevant?

R9: One thing I know is maybe how we at the SOCR team want to see control because we're usually pretty critical with our clients and how they formulate things. So it has to be clear what we're talking about, who is performing the process, and the frequency with which it's performed. I think it's in the playbook of what should be in a good control description. Maybe you can put that framework next to your control descriptions and see am I missing something. This should be in the control to make it more clear for the people performing the controls. So there are a few things that may help improve your framework a bit more, but I think it is already good.

I: All right. Thank you very much. You mentioned the playbook. Where can I find that document?

R9: It's on the SharePoint. But with all the information on SharePoint, it might be hard to find. So I will send it to you.

I: Thanks, that would be great. Now that that was it, I would say thank you for your time.
R9: You're welcome. Glad to help.

Respondent 10: IT auditor at EY (III)

I: All right. Thank you for your time. As I mentioned earlier, I am doing my thesis about the auditability of consortium blockchain. And as explained earlier, I did a couple of interviews with different consortium providers. I made a framework for auditing consortium blockchains with a couple of controls. I drive those controls from frameworks like COBIT, NIST, and ISO, bringing all those relevant controls together. And then what I did is I sat down with different colleagues, my colleagues who are also specialized in blockchain, to filter those controls down to a couple of controls. I came eventually on a couple of controls. Some of them are derived from the frameworks I then tweaked, and others are made up from scratch. And I did a couple of interviews with IT auditors to review and evaluate the control framework. And that is why I also want to sit down with you. I sat down with a fellow IT auditor colleague to discuss from the audit perspective if the control framework is a logical structure or not and what tweaks can be done to the control framework. Eventually, the control framework is for the auditors. So that's why I'm also sitting down with different IT auditors. So I'm going to share my screen which you.

R10: All right!

I: All right. As you can see, I made the control framework here. The structure should speak for itself. I started with the topic. Those topics are derived from academic literature. And then the risks follow; what important risks are there? What are the control objectives suitable for those risks? And what, of course, are the controls that align with those control objectives? And then put the control classification. So is the control preventive, detective, or corrective. And what I do in Column G is I also put the references to the practice. So, where are those controls derived from? And the next follow-up column, I put the reference where the controls or the topic is derived from the academic literature. And eventually, the final column is for the experts, like blockchain experts, or the colleagues from EY like yourself. So if it's allowed, I can put your name, or do you want to be anonymous in the column?

R10: Yeah, that's fine for sure.

I: It's nice beforehand to mention one of the feedback I've, for example, gave was more had to do with more about corrective controls, because what I did, I just made preventive and detective controls. But the other IT auditor colleague also mentioned that corrective is also very important because you can have preventive and detective controls, but if you don't check them up and they are out for that matter, then those preventive and detective controls aren't that effective.

R10: Indeed, actually, for every audit, it doesn't matter if it's a financial IT operation or cyber audit or something. You always have preventive, detective, and corrective controls.

I: All right. So I have to put some corrective controls. What do you think about the overall structure, for example, things in a control framework from your audit perspective or the perspective that are necessary to also mention in a framework?

R10: This looks overall good to me.

I: Okay, nice. Do you also have examples from other frameworks which you work with that have similar structures, for example, or are there other example points that can also be found on those frameworks that you didn't see here?

R10: Within EY, we have frameworks to send to the client that looks quite similar to this one. Those also use more numeric structuring and reference. So maybe you can put that also in your framework. Kind of a numeric reference, but overall it's quite the same for you. We also have a Framework from the IT audit group NOREA.

I: And do we have within SOCR an existing control framework?

R10: Not that I know for sure. You could ask [redacted]. He is the one whom we rely on for that because he is our quality guy. He also creates the controls for the control framework.

I: All right, I noted it down.

R10: I also have a control framework from one of our clients. We have the TSP, which in your case, is the topic. I am going to cross-check the columns for you. You mention the theme, risk control objectives, the control itself, description, and control classification. It seems you mention them all.

I: Oh, that's nice. Is it possible to screenshot the headers and the first row?

R10: Yeah, sure.

I: Okay. That would be nice. That's more for validation purposes. Let's see.

Figure 30

Example Audit Framework

	A	B	C	D	E	F
1	TSP Category	Trust Service Criteria #	Trust Service Criteria description	Control #	Control Description (2022)	Unique / Referral Control
6	Additional Criteria for Availability	A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	A1.2 - control B	Interxion has defined a Group Maintenance Policy for the environmental protections in the data centre and contains a specification of the assets and their criticality, which are subject to planned maintenance. In principal environmental protections receive maintenance on at least an annual basis, however for assets which are subject to condition-based maintenance other maintenance frequencies may apply in accordance with the Group Maintenance Policy and supplier requirements.	Unique
7	Additional Criteria for Availability	A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	A1.2 - control C	Every data centre facility has 24/365 alarm monitoring (Building / DC Monitoring Systems – BMS / DCMS) in place for environmental threats (power supply failures, fire, water leakage hazards, temperature and humidity monitoring) and is monitored by the local Operations team. In addition to the local monitoring, ECSC logs and monitors 24/7 environmental alarms received on the Group Critical Alarm Platform (GCAP) for all Interxion entities to ensure timely response and communication with customers and stakeholders.	Unique
8	Additional Criteria for Availability	A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	A1.2 - control D	For all Busisness critical IT infrastructure, organisation shall take full and incremental back-ups according to approved back-up procedure. The back-ups shall be monitored and after 5 continious back-up failures in one set there shall be an investigation and remediation performed and documented.	Unique
9	Additional Criteria for Availability	A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A1.3 - control A	Disaster recovery personnel perform an annual test of the recovery plan procedures to determine any gaps in capability to meet availability commitments and system requirements.	Unique
10	Control Environment	CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CC1.1 - control A	Personnel are required to read and accept the set of rules outlining the responsibilities and ethics and the statement of confidentiality and privacy practices upon their hire and to formally reaffirm them (at least) annually thereafter.	Unique
	[illegible]	[illegible]	COSO Principle 1: The entity demonstrates a commitment to	[illegible]	Hiring procedures include background checks or reference validation, which are	[illegible]

Note. From screenshot during interview respondent 10.

R10: You can also give a topic and then a number like A1 or the first control of topic Consortium Regulatory Compliance as CRC-1.

I: So, the controls should be numerically named to align more with the topic?

R10: Correct.
I: All right.

R10: As you see, this framework numbers their control in combination with a letter.

I: That's nice indeed. I also see another category in the screenshot related to trust service principles.

R10: Yes, so in your case, that can be seen as a topic.

I: Okay, let's see. One final question I had in mind, which I also previously mentioned to one of the colleagues if I should put a preventive, detective, and corrective measure per topic?

R10: That it is indeed the ideal situation for sure. But it also depends on your control. In SOC 2, you have two types. Type I focuses on the design of controls. There you have mostly preventive, and detective controls. Type II consists mostly of corrective controls.

I: Okay. That's a very interesting point.

R10: So that's a type I. And then, after that, step two is like looking at how it works in periods with sample testing.

I: So to give a clear picture, type I have the preventive and detective controls and the operating effectiveness has only the corrective controls?

R10: Yes, but not always, but most of the time.

I: Could you give an example of preventive, detective, and corrective?

R10: An example of preventive, detective, and corrective would be in the case of fire in a data center. A preventive control would be to close the rooms of the data well so that due to rainy

weather, you would have the water come into the data servers, which could cause a fire, for example. Secondly, a detective measure would be an alarm system to detect the fire. Thirdly, a corrective measure would be the protection system like sprinklers that go off to turn the fire off.

I: All right. I think that was it overall. I wanted to talk more about the structure, and I have much good input, so thank you. I'm going to implement those, and I'm going to tweak those things in the framework. And then eventually, I also talk with other colleagues to see what they have to say.

R10: You should definitely talk to [redacted] He is our quality guy. He has the most knowledge about it. So he knows everything about control frameworks and that kinds of areas. So I think you will be the best person to talk about frameworks.

I: Nice. I'm going to message him to see if we can sit down. All right. Nice. Yes, thanks. I'm going to stop the recording.

Respondent 11: IT auditor at EY (IV)

I: All right. Thank you for joining me. As you can see, I have made a Consortium Blockchain Audit Control Framework. A concept model was built based on interviews with the consortium blockchain providers, literature review, standards, and experts. And what I did is, as explained earlier, I collected all controls, which I thought were relevant from different kinds of frameworks, and I referenced them here. So, the framework logic should speak for itself. I started with the topic, actually, and then the risks. I looked at the control objectives and then, of course, the controls and then the classification of controls which are either preventive detective and/or corrective. And a feedback point from previous meetings I had with IT auditors was that it would also be nice to have a couple of corrective controls examples. So I still have to put those corrective controls in this. And what I did in a column is reference it to practice, the references for the control, and where I got them from, and then, I have a reference to the theory which I collected in my thesis, but I'm going to put it also here from academic papers. And then what I do in the last column, I speak with different kinds of experts to check and validate the logic of the framework and the controls themselves.

R11: Okay, let's start.

I: I ask every participant if you would like to be mentioned in this column, and if anonymously or you want to call by name, it's what you prefer if you want to stay anonymous, as of course, also possible. I just put the function name there.

R11: Let's see. It's okay to put my name.

I: So I have the check by expert column. It's very broad. It's also related to blockchain experts. And then what I talk about with them is just the controls themselves. And then, with it all, I'm more focused on the logic of the framework if it's logically structured or not. Okay, so I based on the framework columns, I based on other frameworks to see if there is a kind of logic or not. A previous feedback point was, for example, when I mentioned that corrective controls were missing, and it would be nice to have them there to give a more logical approach to the control classification. And another feedback point, for example, was that within the SOCR team, for

example, we start with the control objectives. So the risk column, it would be nice to move them to, for example, after the column E. But there were a couple of examples from a feedback point for it all the to perspective. So I also want to focus more on the framework's logic and not so necessarily on the controls themselves.

R11: The setup is good. As for the control objectives, they look more like controls. There is also a standard format for formulating control objectives that you can use. It is as follows: Controls provide reasonable assurance that…[why: subject] maintained in a complete, accurate, and timely manner. Control objectives are more at a higher level. What do you want to achieve with that set of controls? You do not want to have any changes that are unauthorized and could be not tested, not authorized, or not approved. So if we look at the first one and you say, well, it's. The scoping is formally defined, and the line between participants could also be in control. It could also be an actual control that you could test that it's formally defined, that there's a procedure available and that there is alignment between the participants that I don't know based on meeting minutes. So that will be one common. The other one I would say, as we often suggest, clients adding more than one control goes for one control objective. Because if you filled this control, for example, on line two, you would not achieve control objectives. There's nothing left there, no other control that will mitigate the same risk or that could help mitigate that risk. So what we often will set for our clients is, if you have one control, try to change it into a preventive and a detective control. So to give an example, if you have user management and have one control, we are signing excess and revoking access. When people leave, we say, well, at maybe detected control, for example, a review. Do with a monthly review in which you validate that the accounts in there are still assigned to active and breach, that authorizations that are assigned align with the position or function that those people have in the organization. And by doing that, you would more or less mitigate the same risk. So if you, for example, fail the first control, that will fill the second control. So there is no review performed, but at least you could see that authorizations have been assigned under the procedure or authorizations are revoked in line with the procedure. Then the risk might be minimal of that failing control. You could still achieve the control objective. Then you would also need to think, well, what do I want to achieve in the end? And then, just as an example of what I mentioned for change management, you want to ensure that there is no all-through exchange. But the same could be, for example, logical access. Of course, you could have

a lot of different control objectives, but one of them that you often see for logical access you want to ensure that there is no unauthorized access to the application, operating system, or database. And there are a few controls to ensure you will achieve that, that you make sure there is unauthorized access. And that could be true. Assigning access, revoking access, user reviews and all help mitigate the risks related to that control objective to achieve your objective.

I: All right. You mentioned, for example, that for the control objective, it would be good to have a couple of controls for mitigating controls. Did you mean they have to be different classifications, like what should be preventive and what should be detective, for example? Or could it be just multiple controls from the same classification?

R11: Yeah, it could be multiple. However, it depends on your risk. So, you would identify the risk, and you also see often that they make risk classification so that they want to mitigate the risk to an acceptable level. So it might be that you say, well, this control for this risk, but it's not enough to mitigate it sufficiently. So I need a second control, which could also be preventive. I would advise having preventive and detective because if something is going wrong, the preventive part, you would still have a detective part to identify any issues. And if you have two preventive ones, you can have one control failing, but that other preventive control might not mitigate the risk-related risk. So the preventive might fail, and you have another detective in place. So assigning X feels like you have a monthly review in which the manager validates that all the X's assigned is correct. It's a basic sample that mitigates the risk of failing—preventive control.

I: All right. And for control classification, for example, could control also have multiple classifications? For example, one control could be a preventive detective and even corrective? Or is it something you have to be separate for control?

R11: Yeah, I would say it's separate. Let's say you have a preventive part and a corrective part included in one control, and I would suggest splitting them and having the preventive part as one control and the detective as one control.

I: All right. That's a good one. And something which was also mentioned earlier, for example, was to have a couple of corrective controls in it to give it a more structural logic to the framework.

R11: So that's fine. Often you also see that it's also part of the detective's control, but it depends on the process. But to go back to the example about logical access, and you do a review on all the authorizations that are assigned in case you diminish, it does the review, and you find that there is a person in there that's left the organization, the user listing, or there's someone that has authorization signs assigned that they should not have. Then you often see that there needs to be a follow-up—so corrective action. Because you can do a review and find ten exceptions, you still have the risk if you don't do anything with it. You will not mitigate any risk.
So you also see often that there's a corrective part included in the detective control. So you do the review, you find ten exceptions as the one performing the review. And it would be best if you made sure there is a timely follow-up.

I: Okay. So to have a clear picture for me, it is possible to categorize the classifications into two categories, which are, for example, preventive, and then detective & corrective?

R11: That could be possible. You have part detective controls where corrective is part of it. Like the example I was using, you would see the corrective parts. So, detective, you identify ten exceptions, and you need to make sure that you resolve those ten exceptions. And that's the corrective part.

I: All right. Are there other missing important parts within the framework that you would see, for example, in other frameworks that are missing here?

R11: Let's see. Yeah, I would avoid the wording "as a whole" because we're not able to validate all changes for the control. We often use a sample-based approach to be able to come up with "reasonable assurance." So no "full assurance" or "100 percent assurance" that those changes have been approved. Another one, if you scroll down a bit. I don't know if someone already mentioned that. You can use the WHY, WHAT, WHEN, WHO, and HOW formulation. Well, the

“WHY” is clear. You do that to achieve the objective, to mitigate the risk. So that’s clear. But you can also apply “WHAT,” “WHEN,” “WHO,” and “HOW” to the control. So you could say in control, what do they need to perform when so if you say, well, a review needs to be performed, analysis needs to be performed, or an assessment is performed, that’s also based on the risk assessment. Well, how often do they need to perform that? The monthly is the yearly as is the yearly enough. Maybe you say it’s a high risk, so you need to do it at least monthly. And also, who does need to perform the control? So it also helps identify this responsibility of the person in that the organization and what the controls they need to perform.

R11: Also, for us, the clients are responsible, and they need to define the controls, so we cannot write them, write the controls for them. So we say, Well, this is what you need to look at when defining controls.

I: All right. I think I’ve got all the important aspects. So this is just a final review note, an overall quick view of what you just saw. Are there any things that you think would be logical? It would be good to have in it or maybe leave it out.

R11: Let’s see. If I look at line seven, it’s insured. Member skills are available and in the network. You could change it, of course, to more of the wording of the control objective. So our controls provide reasonable assurance that... Only knowledgeable people are involved in the network, for example. They’re the more standard set up standard wording you could use for all of them. I want to ensure that there are no people with insufficient knowledge to work on a network, for example. And some of them are still more control based, so you could even test them. And a control objective you cannot test because you test controls to achieve the control objective.

I: All right. That were all the questions I had in mind for the logical framework. So I don’t know if you have anything else to mention?

R11: No, I think that was it.
I: All right, thank you for your time.
R11: You’re welcome and good luck.

Respondent 12: Blockchain expert at EY (same person as R2)

I: Okay. All right. Thank you for coming. As I mentioned before, I'm actually at the end of the thesis road. I have set up a conceptual framework for auditing consortium blockchain. I've made a Consortium Blockchain Audit Control Framework for Consortium Blockchain. And the key thing was that I had a couple of interviews with different people. The first range of interviews was with consortium blockchain providers, like an interview with B3i, which is a Business-Focused. I spoke with Hyperledger Foundation, and they are purely a Technology-Focused, which is all about providing open-source software and not for commercial use, and R3, which is a Dual-Focused consortium blockchain, which means that they focus on the commercial side of providing software and also they have an open-source platform. So I will share my screen with you with the concept framework. So what I did here was I created the controls derived from different kinds of frameworks, for example, COBIT, ISO, etc.

R12: All right.

I: So the structure speaks for itself. I start with the topic. The topic is derived from academic literature, from different kinds of theories. Then I'm going to start with the risks, then the control objective, and then the controls. And then, I state the control classification, which is either preventive, detective corrective, and then in columns (G), (H), and (I), which is specifically important for my thesis. I mention, of course, a reference to practice. So, where do those controls derived from or inspired from which standards they are. Column (H) references academic theory. So I try to connect the practical information with the theoretical academic literature. And then, of course, in the final column (I): check by an expert, I mentioned the people who like validated or reviewed my controls. And I asked every person I interviewed if they wanted to be mentioned by name or to stay anonymous. I don't know what you prefer? I can also state just your function and that you work at EY?

R12: I would personally prefer to stay anonymous If you don't mind.

I: All right, I will mention it as an anonymous check. Going back at the framework. I provided a couple of risks, the control objectives, and the controls. And what I did is I stated per topic three

types of controls: preventive, detective, and corrective, to show the logical structure of going from preventive to corrective. So the result is this framework. As mentioned earlier, this is, of course, a conceptual model. It is to show that there is a need, which hopefully forms a basis for further research and development of a simple framework for new. So what I want to start is, first of all, with the logical structure of the framework. If you look at the framework briefly, do you think it is a logical structure? Do you think there are key points that are missing in the structure of the framework?

R12: Well, if I look at the risk control matrix, that's mostly provided by clients. Of course, there are a couple of important things, such as reading the topic, for instance, or the risk that it's trying to mitigate. Then, of course, the control objective and then the actual control. So yeah, that's very logical. When I look at more leveled risk & control frameworks, you always have the function of the person executing the control and stakeholders, but I don't think it is necessary for your framework. And as auditors, what we're trying to do is we're trying to look at risks and see what we can do to mitigate those risks. So the starting point is always a risk. You have three main processes: manage access, manage change and manage operations. There are certain specific risks formulated by EY worldwide that are mentioned in the global audit methodology. And those risks are always like the starting points for basically everything. Every risk applies to every situation and organization, but it is a starting point. So I would say this is the correct order. So you did it correctly, in my opinion.

I: Well, thanks. I also talked with a quality person from the SOCR team who has experience building frameworks. And one thing he mentioned was, and I think that has to do with his own way of working because he mentioned there isn't specifically a standard for it, but maybe you in your team have a specific way of formulating it. But he mentioned that there is a standard way of formulating control objectives. Every sentence starts with the same, like a couple of words, and then you state your own control or the control objective themselves. Is that also a way of working in your team?

R12: Yeah, it sounds logical. I'm not familiar with it, to be honest, but what mostly happens is that we get a risk control matrix or framework from our client, which is their own risk and control

framework. So obviously, we can say everybody's control objective is formulated incorrectly, but generally, they format their controls and control objectives. And that's what we look at. Of course, we have improvements, but in general, I'm not familiar with this, but I can see that it's a logical way of working because it gives more structure to what you're doing.

I: Okay. Yeah, that's logical. One thing that pops to my mind is actually, is there anything crucial or, from your perspective, anything you would see like you would like to see in the framework? So the necessity, the basic things are in the framework already you mentioned, but are there something which would be nice to have in the framework?

R12: So, during my own thesis, I wrote about blockchain and the risk controls arising from blockchain. I always compared what we have in the regular IT environments that we know right now. That's something to do with network effects of governance, this kind of stuff. So I see you're working a lot here with the topic. So a little more elaboration on what has already been written in the idea as we know it and the blockchain part and what are the make comparisons saying, all right, this is what we already know, and this is headed specifically for blockchain for this, this reason to give a better understanding to people who are not that familiar with blockchain. Of course, quite a lot of work says you're not going to do it, but that would make it better from my perspective.

I: Okay. So what I just did in my thesis indeed was actually what you mentioned. So I'm happy to hear that I made the comparison. Also, I forgot to mention is from those interviews I had with the consortium blockchain providers, one of the main things that came forward was that most issues arise from off-chain. Off-chain you can broadly define it as everything that's not on the blockchain. It could be hardware, software, or everything from the individual node. The issues they face are the bridge between on-chain and off-chain, called the Oracle. So something can happen on the transaction, on the blockchain, which is correct, but maybe something wasn't correctly done in the real world. So long story short, the issues are off-chain related. And one of the things that can be done is to have good governance practices. So that's why I focus more on the governance aspect and the off-chain related controls.

R12: Indeed, I think one of the major problems with blockchain is the connection between the on-chain and the off-chain processes.

I: Okay. Is there anything else you want to mention? Otherwise, I think what's good for a follow-up is just that I'm going to finish this, and maybe if you want for yourself a copy, of course, you can have that?

R12: Yeah. Sounds good. So I look at the paper now. Of course, I haven't read it in detail. Yeah, I can imagine. That's not everything that you've written down is relevant. Maybe some things are missing, so I'm happy to take a look at it when I have time. I'm not sure if it will be possible before you hand it in, because I have quite a busy week at the moment and I'll be on holiday next week.

I: I am following the design science research procedures for creating artifacts. You'll have requirements, the requirements phase you collect, and the requirements you want to have in your framework, which I did. You got to develop it. You're going to review it, and in the end, there is a communication phase in which you hand the publication over to the organization. So because one of the first talks was with you, I thought maybe it's good for the communication phase to hand this framework over to you as a more formal thing.

R12: You can hand it over to me. I'm quite interested in this to look at it in detail. But as I mentioned, of course, looking from a time perspective, I have three days before going on holiday. So from that perspective, I think for you at the moment, but I'm certainly interested in taking a more detailed look at your framework and thesis. So in retrospect, of course.

I: All right. Thanks. I don't have any more questions. I think I've got all the points discussed. I don't know if you have any additional questions for me?

R12: Yes. So when we look at a consortium blockchain, right. It's a very interesting type of blockchain that you also, somewhere in your thesis, built like a little bridge to, let's say, a public blockchain or a strictly private blockchain and, well, to dive a little bit deeper in. That's to show

what the difference is and also like the statement, which is, I would say an exclusion. That's because the blockchain is not all the same as a public blockchain, for instance, so the results from the framework should not be interpreted as such. I mean, that's an important thing to mention. I would also be well, maybe for a follow-up. I'm not sure if you did that, but yeah. Of course, you're not going to do that. But yeah, so I'll mention that it will be nice, I think.

I: I did this as part of the literature review. What I did is I started first of all with network-related theories like actor-network theory and stakeholder theory. From there, I want to address some important key elements to this to later explain what consortium blockchain is from an academic perspective and then from consortium blockchain. It's in content and detail itself. I just made the yeah and briefly mentioned the differences between the private-public and the consortium. But I didn't go into detail about that part because many research articles already mention the different types of blockchain and their impact. So I thought maybe, in that sense, it's going to be overdone. So I briefly mentioned and gave them more of a summary of those articles to build my view of my part. But if you're interested in specific detailed differences and what kind of impact they have, I have a couple of articles. Maybe I could send them to you if you want?

R12: Yeah, sure, that would be nice. And, of course, your thesis. Or I can also take a look at it and define specific chapters. But the reason why I'm saying this is it's because when I was writing my thesis, first of all, I thought blockchain was just blockchain. But yeah, there is so much there are so many differences in all of those sorts of blockchain. So it's very important to mention that and articulate what kind of blockchain you're operating in because blockchains are different sorts of resources, and blockchain if you go a little further. So that's just something I would.

I: Oh, that's good; that's a very interesting point you mentioned because that's specifically to consortium blockchain. They have briefly mentioned that there are three types in which I also categorize my interviews. They have business-focused that, is commercial use purpose only. The technology-focused, which is focused on open-source software and providing it freely. And then you have the dual-focused, which provides open-source and commercial purposes. But there isn't much information to find about that. So I'm going to write in my future research something about

that for people who want to research that further because there isn't much information in categorizing consortium blockchain specifically. And one of the reasons had to do with I talked with one of the guys on Hyperledger. They said, yeah, there isn't a specific categorization because it's a very dynamic world, like what can be considered now being a business-specific could also be like next year be dual-focused or technology-focused. It's just that the classification wouldn't add any real value in that sense. So there isn't much information to find about the specific category.

R12: Of course. And what's also important to mention then is that if you look at risk can be applicable for all sorts of blockchain areas or even for all the blockchains in general. So if you make your framework, it's also something to consider. But now, if I'm looking at this, I think you did a good job. I think you learned quite a lot. The last time I spoke with you, you were less knowledgeable about blockchain.

I: Thanks, I really appreciate it.

R12: It's a great job. Yeah. We'll be very interested to see what you come up with. So please send me your work and then take a look at that a little bit later. All right. Now, good luck with finishing up your thesis. And if you need anything more, I won't be able this week but to help you. But of course, we'll catch up later.

I: I will; thanks for your time and have a good vacation.

Appendix B: Profiles

Audit Firm Profile

Table 13

EY Profile

Categories	EY
Industry	Professional services
Founded (Post Merger)	1989
Headquarters	London, England, UK
Chairperson	Carmine Di Sibio
Services	Assurance Consulting Tax Strategy and Transactions
Revenue	$40B
Number of Employees	312,250
Website	https://www.ey.com

Consortium Profiles

Table 14

R3 Profile

Profile	R3	
Type of Consortium	Dual-Focused	
Founded	2014	
Headquarters	London, England, UK	
Executives	Founder & CEO: Co-Founder & CPO (Chief Product Officer): CIO: CTO: CCO (Chief Communication Officer): CRO (Chief Revenue Officer): Chief Engineering Officer:	David E. Rutter Todd McDonald James Carlyle Richard G Brown Charley Cooper Cathy Minter Dave Hudson
Team Size	250-500	
Products	Corda DLT - Corda Network – Conclave	
Social Media	LinkedIn – Facebook - Twitter - Instagram	
Website	https://www.r3.com/ https://www.corda.net/ (DLT product) https://corda.network/ (Network product) https://www.conclave.net/ (Cloud product)	

Table 15

Hyperledger Foundation

Profile	Hyperledger Foundation	
Type of Consortium	Technology-Focused	
Founded	2016	
Headquarters	San Francisco, California, United States	
Executives	Executive Director: CTO: Senior Director of Community Architect: Director of Ecosystem: VP, Asia Pacific, Hyperledger and OpenSSF: Operations Manager:	Daniela Barbosa Hart Montgomery David Boswell Karen L. Ottoni Julian Gordon Min Yu
Team Size	51 - 100	
Products	Hyperledger Indy - Hyperledger Fabric - Hyperledger Iroha - Hyperledger Sawtooth - Hyperledger Besu	
Social Media	LinkedIn – Facebook - Twitter	
Website	https://www.hyperledger.org/	

Table 16

B3i Profile

Profile	B3i		
Type of Consortium	Business-Focused		
Founded	2018 The Linux Foundation		
Headquarters	Zürich, Switzerland		
Executives	CEO: CFO: CPO (Chief Product Officer): CTO: CoS (Chief of Staff): Head of HR: Finance Manager: Chief Architect:	John Carolin Patrick Crass Antonio Di Marzo Iryna Zhovtobryukh Linda Costabile Alexandre Erard Mark Tickle Alessandro Spadoni	
Team Size	11 - 50		
Products	**Platform**	**Application for Reinsurance**	**Application for Commercial**
	B3i Fluidity	B3i Re	Climate Risk Models
		Eurapco Unity	MGA
		Pools	
Social Media	LinkedIn - Twitter		
Website	https://b3i.tech/		

Profile 1: R3

Background

Founded in 2015 as an initiative by nine banks (and now backed by over 60 banks), R3 provides business technology and services for regulated industries where trust is critical. Through their platforms, multi-party solutions can leverage the 'Power of 3'which merges R3's trust technology, connected networks, and regulatory market expertise to drive market innovation while also enhancing financial services sector operating processes. R3 is also the first firm to provide both a private, secure, and scalable distributed ledger technology platform specifically designed for regulatory markets and a confidential computing platform (R3, n.d.).

Business Goals

- Trust Technology: R3's platforms allow the creation of solutions that create and offer confidence between parties since they are built on distributed ledger technologies (Corda Network, n.d.).
- Connected Networks: R3 has created a massive ecosystem of diverse stakeholders from financial businesses and regulators to tech companies. As a result, customers and partners may use pre-established consortia, operational and governance procedures, and network assistance(Corda Network, n.d.).
- Regulated Markets Expertise: Only R3 has market access and deep industry expertise to help firms accelerate the development of next-gen multi-party solutions that deliver trust for participants across regulated industries (Corda Network, n.d.).

Products

Corda Network: Network of participant entities interoperating with each other. The Corda Network consists of: nodes (participants), an identity service, a network map service (that publishes information about how to connect to nodes on the network), one or more notary services, and zero or more oracle services (Hearn & Brown, 2019).

The Corda Network is governed by the Corda Network Foundation which is a Dutch non-profit organization founded in December 2018. The Corda Network Foundation board consist of eleven members where nine of them are participants, and the other two are chosen by R3 (Corda Network, n.d.).

Corda: *"A distributed ledger platform for recording and processing financial agreements, designed to implement the vision contained in this document".* (Brown et al., 2016).

Conclave: *"A platform for the rapid development and execution of 'privacy-first' applications; and a set of privacy-first cloud services that are themselves built using the Conclave platform".* (Brown, 2021).

Profile 2: Hyperledger Foundation

Background

The Linux Foundation launched Hyperledger in December 2015 with the cooperation of major industry giants including IBM, Intel, and SAP to facilitate the collaboration of distributed ledgers based on blockchains. Open-source blockchain technology was created by combining the efforts of these companies. Because of organizations like these, blockchain is on its way to becoming a widely used and industry standard technology. Hyperledger has more than 230 members, 10 projects with 3.6 million lines of code, and 10 active working groups; and close to 28,000 individuals who have attended 110+ events throughout the globe (Blummer et al., 2018).

Business Goals

Hyperledger Foundation has the following five goals:

- *"Create enterprise grade, open source, distributed ledger frameworks, and code bases to support business transactions".*
- *Provide neutral, open, & community-driven infrastructures supported by technical and business governance".*
- *Build technical communities to develop blockchain and shared ledger Proof of Concepts, use cases, field trials, and deployments".*
- *Educate the public about the market opportunity for blockchain technology.*
- *Promote our community of communities taking a toolkit approach with many platforms, and frameworks".* (Hyperledger Foundation, n.d.-a).

Products

Hyperledger facilitates and encourages the development of a variety of enterprise distributed ledger frameworks and hosts the below open source distributed ledger frameworks:

Indy: Blockchain-based tools and frameworks, as well as reusable components, for establishing online identity that may be used across variety of compartment (Hyperledger Foundation, n.d.-b).

Fabric: Serves as a basis for constructing modular applications by enabling plug-and-play components like as consensus and membership services which allows it to be used in a wide variety of industrial applications (Hyperledger Foundation, n.d.-b).

Iroha: A simple-to-use, modular distributed blockchain with its own proprietary consensus algorithms, a comprehensive role-based authorization mechanism, and support for multi-signature transactions (Hyperledger Foundation, n.d.-b).

Sawtooth: For the creation, deployment, and management of distributed ledgers. A new consensus mechanism called PoET (Proof of Elapsed Time) is included for targeting large dispersed populations while using minimum resources (Hyperledger Foundation, n.d.-b).

Besu: This Ethereum client is enterprise-ready and supports both public and private permissioned network use cases. Its sophisticated permissioning systems are intended for usage inside a consortium (Hyperledger Foundation, n.d.-b).

Profile 3: B3i

Background

B3i (Blockchain Insurance Sector Initiative) intends to enhance the insurance sector by constructing a network architecture and a platform that allows the execution of protocols that decrease and eventually remove administration. There are presently approximately 40 enterprises in the B3i Services AG network that is owned by 21 large insurance companies like Achmea, Aegon, Africa Re, Ageas, Allianz, AXA, CPIC, Deutsche Rück, Generali, Hannover Re, IRB Brasil RE, Liberty Mutual, MAPFRE RE, Munich RE, SBI Group, SCOR, Swiss Re, Tokio Marine, Türk Reasürans, VIG Re, and Zurich from five different continents. In October 2016, B3i was established as an insurance sector consortium, creating a platform and protocol to meet important insurance industry requirements by expanding its network and partnering with other firm and sector projects around the globe (B3i, 2021).

Business Goals

- *"Create a DLT based network through the adoption of standardized systems and protocols*
- *Through the network, enable the market to optimize processes and capital allocation and generate significant cost savings.*
- *Offer network users a variety of integrated applications from B3i and partners".* (Roberts, 2022).

Products

B3i Fluidity (Platform):	An insurance industry platform that provides services and modules for the creation and distribution of linked applications on the B3i network (B3i, n.d.-c).
B3i Re (App):	Is an reinsurance application that facilitates the end-to-end digital transformation of the reinsurance industry by allowing brokers, insurers, and reinsurers to collaborate extensively to ensure that it satisfies all standards and delivers value to all stakeholders (B3i, n.d.-f).
Eurapco Unity (App):	An industry-led worldwide initiative consisting of a strategic partnership between eight mostly cooperative European insurers and B3i Services AG, which split risks amongst the network (B3i, n.d.-b).
Pools (App):	A DLT based solution to efficiently manage inter and intra nuclear pool reinsurance contracts which results cost- and time reduction spent on administrative activities (B3i, n.d.-e)
Climate Risk Models (App):	A cooperating between B3i, TCS and an Open Source catastrophic modeling platform in order to assist banks and financial institutions comply with new environmental regulations (B3i, n.d.-a).
MGA (Managing General Agent)	A protocol that provides the seamless linking of end-to-end workflows by enhancing current IT infrastructures with standardized data dissemination and expandable network connections (B3i, n.d.-d).
Data Protocol (App):	

Appendix C: Consortium Nodes

R3

Table 17

R3 Nodes

Founding Member	Partnership	Member	Technology	Assist
Banco Bilbao Vizcaya Argentaria, S.A.	AlphaPoint	Société Générale Blockchain	4Linux	TokenSoft
Barclays	Bond180	3i-Infotech	7COMm	11:FS
BBVA	Hex Trust	ABN AMRO Digital Impact Fund	Accenture Blockchain	
Commonwealth Bank of Australia	HSBlox	Accuarion	Adaptive	
Credit Suisse Blockchain	Infosys Finacle	Accuity	Agora Digital Capital Markets	
First American	MobiFi	AIA	alabus ag	
Hyperledger Foundation	Satoshi Systems	Ailancy	Alfa Bank Blockchain	
Marco Polo	SWIFT Blockchain	Akoncepts	Amalgam Inc.	
Royal Bank of Scotland		Allied Irish Bank	Amazon Web Services (AWS)	
State Street		American International Group	amplicade GmbH	
UBS Blockchain		ARSOKOS Corporation	AOS SaS	
		Ashurst LLP	Appway	
		ATB Financial	Archax	
		Avasant	At.Cash	
		AXS	Ateon (Alhamrani Universal) CO.	
		B2X Central	Attinad Software Inc.	
		B3i	Avocado Blockchain Services	
		B9lab Ltd	aXpire	
		Bain & Company	AyanWorks	
		Banca Mediolanum	B3	
		Banco Bradesco S.A.	BBChain	
		Banco de Crédito del Perú	BCDLTSolution	
		Bangkok Bank Public Company Limited	BCS Technology	
		Bank ABC	BCSIS	
		Bank of America Blockchain	Blanc Labs	
		Bank of America Merrill Lynch	Block8	

		Bank of Communications (Hong Kong) Limited	Blockchain Worx	
		Bank of Cyprus	BlockSpaces	
		Bank of Montreal	Blocksure	
		Banks Itaú Unibanco Holding SA	Bloxian Technology	
		Banorte-Ixe Securities	BNY Mellon	
		Baringa Partners	Bolero	
		BCI	BSOS	
		BCS Consulting	Business Blockchain	
		Bearing Point	CAC Corporation	
		Blockchain Education Club	Calypso	
		Blockchain Healthcare Review	Canonical	
		Blockchain Research Lab - University of Zurich	Cegeka	
		Blocklime	Celadon	
		BNP Paribas SA	Chain Ninja	
		Capgemini	Chainhaus	
		CFETS	ChainNova	
		Chappius Halder & co.	Chainstack	
		Chatsworth	ChainThat	
		China Merchant Bank	China Systems	
		Chorum	Chinsay	
		CIBC	Cieloblu Group	
		Citi Group	CleNET Technologies	
		Clifford Chance	CMA	
		CLS LedgerConnect	CodeIT	
		Cognizant Technology Solutions	Coinplug Inc	
		Commercial International Bank S.A.E	CommodDT	
		Commerzbank AG	Contour	
		Cordite Foundation	Convexium	
		CTBC Bank Co., Ltd.	Crowd Machine	
		Danske Bank A/S	CryptoBLK	
		Dapps Inc.	CTIA	
		Davivienda	CULedger	
		DAVOS Custody	Custom Blockchain Solutions	

		Deloitte Blockchain	CYBAVO	
		Deutsche Bank AG	DactaTrace.swiss	
		Deutsche Börse Group Blockchain	DASL (Digital Asset Shared Ledger)	
		Dianrong	DataArt	
		DLT Program @ING	DataLakers	
		DNB Bank	DDS Soft	
		Electi Consulting Ltd.	Deal Technologies	
		elphi, Inc.	Deon Digital	
		Ernst & Young Blockchain	d-fine	
		everis	Digiledge	
		FABERNOVEL Singapore	Diginex	
		Fitzner Blockchain Consulting	Digital Ventures	
		Flint Global	DreamzTech Solutions Pvt. Ltd.	
		Geekologue	DrumG Technologies	
		Hashcorp	DTCC Blockchain	
		Hedgebase	EBCS	
		Hiscox	eMALI.IO	
		HOBNOB	Enterprise SPA	
		HSBC	Envision Blockchain Solutions	
		I Am Consulting	Equinix	
		Infosys Limited	essDOCS	
		ING Group	E-Title	
		Kasikorn Bank	EUROchain	
		KB Financial Group Inc.	Everledger	
		KEB Hana Bank	Evernym	
		Kerala Blockchain Academy	Exactpro Systems	
		KPMG International Cooperative	Exprivia	
		Krung Thai Bank	Ezly Tecnologia	
		LCUC	fifth9	
		LimeChain	Finastra	
		Lloyds Banking Group	Finchain / Flow Representações S.A.	
		Macquarie Group Limited	FinFabrik	
		Mazars	Finteum	
		Micobo	Fluyd	

		Mitsubishi UFJ Financial Group, Inc.	Fornax Tecnologia	
		Mizuho Financial Group	Gemalto	
		National Bank of Canada	GFT Technologies SE	
		National Bank of Egypt	Giant Machines	
		Natixis	Giesecke+Devrient GmbH	
		NatWest	GoBlockchain	
		NH Financial Group	Google	
		Nomura Holdings, Inc.	GROW Super	
		Nordea Bank Abp.	Guardtime Blockchain	
		Northern Trust	GuildOne	
		ObjectFrontier Inc.	HPE	
		ObjectTech	HQLAx	
		OP Financial	HSBlox	
		OUE Limited	Huawei Technologies Co., Ltd	
		Paris EUROPLACE	IDWorks	
		Parsec	Imprint Blockchain Services	
		Ping An Insurance	Industria	
		PNC Bank	Instimatch	
		Post Oak Labs	Intel	
		Propine	IntellectEU	
		Protiviti	Intellica	
		PwC	Interswitch Limited	
		Qiwi	Interxion	
		Quinlan & Associates	IPC Network Services	
		Raiffeisen Bank International (RBI)	IPN Group	
		RCI Banque	ISID	
		Refinitiv Japan K.K.	JDX	
		RiskStream Collaborative	K2 Partnerning Solutions	
		Royal Bank of Canada	Kaleido	
		Saudi British Bank	KI decentralized	
		SBI Bank LLC	Kratos Innovation Labs	
		SEB	LedgerBlocks	
		Shinhan Bank	LG CNS	
		Smart Communications	LoanXchain	
		SMBC	LongHash	

		SMT Soluções	Lucid-IS	
		SnapCheck	Lutech	
		SoftServe	Luxoft	
		Sovrin	Magia Digital	
		Standard Chartered	MasterCard	
		SunTrust	Matrics	
		SwapsHub	Methods	
		Synchrony Financial	Microsoft Corporation	
		Synpulse	MonetaGo	
		Talan	MonetaGo	
		Targens	Monetary Authority of Singapore	
		TCS	MoneyGram	
		Tech Mahindra	Mphasis	
		Temasek	Multichain Maestro pte Ltd.	
		Thanachart Bank	Multiledgers	
		The CareVoice	MV37	
		ThoughtWorks	Nasdaq, Inc.	
		TIBCO Software Inc.	NEC Corporation	
		TigerRisk	NIIT Technologies	
		TipoTapp	NorBloc	
		TIS Inc.	NorthChain	
		Tradecloud	NPP LTT	
		US Bank	NuWave Technologies	
		Vaco San Francisco	OCTO Technology	
		Vesl	OmniPayments	
		Westpac Group	OneKey	
		Wethaq	OpenCrowd	
		Woori Bank	Oracle	
			Oraclize	
			PCCW Solutions	
			Persistent Systems	
			Piston Vault Pte. Ltd.	
			Pitang	
			Pivotal Technologies Limited	
			PixelPlex	
			ProCredEx	

			Project Inthanon	
			Publicis Sapient	
			Quisitive	
			Resource	
			SafeXain	
			Schrocken	
			SDX SIX Digital Exchange	
			Seal Chain	
			Securosys	
			Sempre IT	
			Servntire	
			S-labs	
			Solace Systems	
			Spunta	
			Stefanini	
			SWIFT Blockchain	
			Swisscom Blockchain	
			Synechron	
			Tag Loyalty Inc.	
			TAKING Results e Informática Eireli - EPP	
			Tango IT	
			Tech29	
			Teknolojia	
			Tieto Blockchain	
			Toptal	
			Total Technologies and Solutions FZ-LLC	
			TradeIT Global (Pvt) Ltd	
			TradeKey.com	
			Tradewind	
			Tradle	
			Truefact Technologies Limited	
			unchain.io	
			UST Global	
			Utimaco	

			Vassu Tech Services Inc.	
			Vyoma Software	
			Wall Street Blockchain Alliance	
			Webmob Software Solutions pvt ltd.	
			Wells Fargo Blockchain	
			Wipro Limited	
			Wizeline Inc.	
			WorldSibu	
			XENIRO Ltd.	
			Yokiki	
			Zensoft	
			ZirconTech	

Hyperledger Foundation

Table 18

Hyperledger Foundation Nodes

Founding Member	Partnership	Member	Technology	Assist
ABN AMRO Digital Impact Fund	Walmart China	33.cn	Accenture Blockchain	TokenSoft
Accenture		AAIS	BlocWatch	
Blockchain Capital		Accord Project	BSOS	
BNY Melon		Aetna	EMURGO	
Calastone		Airbus	Snapcert	
Cisco		Alibaba Blockchain Cloud	Snapper Future Tech	
CLS LedgerConnect		Altoros		
CME Group		American Express		
ConsenSys Mesh		Amihan		
Deutsche Börse Group Blockchain		Ankr Network		
DTCC Blockchain		Auburn University		
Fujitsu		Australia And New Zealand Banking Group Limited (ANZ)		
Guardtime Blockchain		Avanza Innovations		
Hitachi		B9lab Ltd		
IBM Corporation		Baidu AI Cloud		
IntellectEU		Bank of England		
Intellectsoft		BBVA		
JPMorgan Chase & Co.		Big Tree Finance		
Linux Foundation		Bitfury Holding B.V.		
NEC Corporation		Bitmark		
R3		BlackRidge Technology		
RedHat		Blinking		
State Street		Blockchain at Berkeley		
SWIFT Blockchain		Blockchain Research Institute		
Symbiont		Blockchain Technology Partners		
VMware		Blockchain Training Alliance		
Wells Fargo & Company		BlockDAO		
		Blockforce Capital		
		Bloq		
		Bosch		

		British Columbia Ministry of Citizens' Service		
		Broadridge		
		BSOS		
		BTS Digital		
		BUDAPESTI MŰSZAKI		
		Business Telecommunications Inc.		
		CAICT		
		Cambridge Centre for alternative Finance		
		Capgemini		
		Cardstack		
		Cargill		
		CERTH		
		ChainDigit		
		ChainYard		
		Chamber of Digital Commerce		
		Change Healthcare		
		Chengtay		
		China Merchant Bank		
		China Minsheng Bank		
		China Securities Credit Investment		
		China Systems		
		Circulor		
		Citi Group		
		Clause		
		Cloud Security Alliance		
		Cognition Foundry		
		Coil		
		Coinplug Inc		
		Collegium Da Vinci		
		Consensus Datatrust		

		Construction Blockchain Consortium		
		CPQD		
		CULedger		
		Daimler		
		Dealer Market Exchange		
		Deloitte Blockchain		
		Deutsche Bank AG		
		Dianrong		
		Digicert		
		Digital Asset		
		DLT Labs™		
		DocBloxs		
		ElamaChain		
		Elemential		
		Elementrem		
		Embleema		
		Enterprise Ethereum Alliance		
		Estateably		
		Evernym		
		Exactpro Systems		
		Experian		
		Federal Reserve Bank of Boston		
		Fedex		
		Filament		
		FinFabrik		
		Flowchain		
		FNZ		
		ForFirm		
		Forgerock Inc.		
		Forms Syntron		
		frst		

		Fusion Tech		
		Globlue		
		GLOSCAD		
		GS1US		
		H3C		
		Healthverity		
		Hedera Hashgraph		
		Honeywell		
		Huawei Technologies Co., Ltd		
		Hunan University		
		Hyperchain Capital		
		Identity Foundation		
		InBlock		
		India Ministry of Finance		
		Information Technologies Institute		
		Infrachain		
		Inspur		
		Intain		
		Intellectsoft		
		International Computing Centre		
		INUIT Fondazione		
		Investrata Foundation		
		Iownit		
		IPChain		
		Jitsuin		
		KEB Hana Bank		
		Kerala Blockchain Academy		
		Kiva		
		KompiTech		
		Korea Securities Depository		
		KoreConx Inc.		

		koscom		
		KRX Korea Exchange		
		KrypC		
		Lares		
		LedgerDomain		
		Lenovo		
		LG CNS		
		Lilly		
		Limar GLobal		
		Loyyal		
		Majid Al Futtaim		
		Medicalchain SA.		
		MediConCen		
		Mercy Corps		
		Microsoft Corporation		
		Milligan Partners		
		Ministerstwo Cyfryzacji		
		Mintree		
		MIT Connection Science		
		MobileBridge™		
		Monax Platform		
		Monetary Authority of Singapore		
		Moscow Exchange		
		Murphey & McGonigle		
		myndshift		
		National Association of Federally-Insured Credit Unions		
		National Association of Realtors		
		Nexiot		
		NorBloc		
		Nornickle		

		NuCypher		
		Omnitude		
		Optherium		
		Oracle		
		OSCRE		
		Paramount Software Solutions		
		PDX		
		Peer Ledger		
		PeerNova		
		PeerSafe		
		Peking University		
		Penn Blockchain		
		POINTS		
		Portland State University		
		Posteitaliane		
		Pravici		
		Pro Insight		
		Produce Marketing Association		
		PwC		
		Quant Network		
		RealMarket		
		Regov Technologies		
		Ripple Labs Inc.		
		Salesforce Blockchain		
		Samsung SDS		
		SAP		
		Sberbank of Russia		
		ScanTrust		
		Scroll Network		
		Secure Key		
		Securitize		

		sedna		
		Silicon Valley Bank		
		Smart Blockchain Laboratory		
		Smart Dubai		
		Smart Link Labs		
		Soramitsu		
		Sovrin		
		SPB		
		Spinsys		
		splunk		
		State Farm		
		Sun Yat-Sen University		
		Swisscom Blockchain		
		Syncsort		
		Tecnalia		
		Tencent Cloud		
		Thales		
		The Illinois Blockchain Iniative		
		Think Tecture		
		Tierion		
		T-Labs Blockchain Group		
		TNO		
		Trade Finance Registry		
		Truffle		
		Truthso		
		UCLA Blockchain Lab		
		UltraChain Tech		
		Unbound Tech		
		University College London		
		University of Nicosia		
		USC Viterbi		

		Vilnius Gediminas Technical University		
		VisibleSCM		
		Visma		
		Vitalhub		
		VSP Global		
		Wall Street Blockchain Alliance		
		Wanchain		
		we.trade		
		Wipro Limited		
		Xiaomi Corporation		
		Xilinx		
		Xooa		
		Yale		
		ZC Research		
		Zheijian University		
		Ziggurat		

B3i

Table 19

B3i Nodes

Founding Member	Partnership	Member	Technology	Assist
China Pacific Property Insurance Co., Ltd. Shenzhen Branch	Ritablock	Liberty Mutual Group		
Munich Reinsurance		R3		
Swiss Re				
Allianz SE				
Tokio Marine Holdings				
VIG Re				
Deutsche Ruckversicherung AG				
SBI Ripple Asia				
Aegon				
Ageas				
Zurich Insurance Group				
AXA				
Scor				
Achmea				

Appendix D: Code Scheme

Code Scheme Overview Version

Figure 31

Coding Scheme Overview Version

	Audit & Assurance 40	Blockchain 98	Governance & Struct... 51	Network/Consortium 78	Off-Chain 27	Totals
1: Respondent 3.docx 108	4	11	28	32	1	76
2: Respondent 4.docx 94	5	34	17	6	4	66
3: Respondent 5.docx 96	8	8	1	13		30
4: Respondent 6.docx 83		12		14	15	41
5: Respondent 7.docx 25	3	6		3	2	14
6: Respondent 8.docx 39	3	13		1	5	22
7: Respondent 9.docx 49	5	3	1	5		14
8: Respondent 10.docx 9	1					1
9: Respondent 11.docx 42	3			1		4
10: Respondent 12.docx 20	2	5	1	1		9
11: Respondent 1.docx 11	3	1	1			5
12: Respondent 2.docx 22	3	5	2	2		12
Totals	40	98	51	78	27	294

Code Scheme Detailed Version

Table 20

Coding Scheme Detailed Version

Respondents	● Audit & Assurance Gr=40	● Blockchain Gr=98	● Governance & Structure(s) Gr=51	● Network/Consortium Gr=78	● Off-Chain Gr=27	Totals
Respondent 1 Gr=11	"We explain to the participant the standard development process and how they can participate in contributing their ideas about a standard and making agreements with stakeholders in their field" "NEN can support EY in initiating new standardization projects around blockchain auditing. EY can also participate in ISO groups via the NEN blockchain standards committee" "In order to guarantee that DLT-based systems are properly audited, a proposed guidance note would specify the domains to be audited and offer possible approaches."	"In the field of blockchain auditing, an ad hoc group was established in 2020 (ISO/TC 307/AHG 2 Guidance for Auditing DLT Systems)"	"The primary goal of TC307's work is to provide standards for DLT-based system installation, risk detection, and governance."	0	0	5

Respondent 2 Gr=22	"To ensure system design and stability, certain users may need assurance that the blockchain service (private /permissioned) or the new platform they are moving to is safe and secure." "For a private DLT to be successful over the long run, an impartial, trustworthy third party must certify that the controls are functional. Thats where we come into play." "Before giving access to the DLT systems, a the audit party will be in charge of performing identity checks and authenticating users' credentials."	"Business Continuity and Disaster Recovery – Private / permissioned blockchain has centralized and decentralized components. There needs to be a concrete understanding of what will happen should these components be affected by any potential factors." "To ensure system design and stability, certain users may need assurance that the blockchain service (private /permissioned) or the new platform they are moving to is safe and secure." "Identify and manage blockchain risk, which might have a significant reputational and/or financial effect." "Provide management with a comprehensive view of blockchain technology that encompasses technical and non-technical aspects" "It may also enforce and monitor the blockchain protocol for security reasons. When a node hosts this service, the confidence among other nodes decreases."	"Network & node governance - Monitoring network for information compliance and node reputation checks to handle and resolve disputes." "In addition, a comprehensive DLT audit would provide the organization's governing board confidence"	"Interoperability & Integration - Consistent communication between multiple network participant platforms and enterprise legacy systems" "Network & node governance - Monitoring network for information compliance and node reputation checks to handle and resolve disputes."	0	12

Respondent 3 Gr=108	"We have all of the big four companies or actually divisions of them in our network: Deloitte Blockchain, Ernst & Young Blockchain, KPMG International Cooperative, and PwC." "But they aren't there necessarily to audit nodes or the network, but more to gain from the network knowledge and then provide their services to their customers" "As for auditing the network, our Corda DLT solution provides traceability of the records on the blockchain." "It provides transparency to the network where each node can audit the chain for themselves"	"Corda Network is a network of 'nodes' or identities that allows fast, safe, and private transactions using Corda software" "Whereas, a smart legal contract is a smart contract that has progressed to the point where it is considered a legally final and binding agreement." "'Self-contained governance' means that there is no need for an outside expert to provide guidance on a blockchain transaction's rules or how to deal with any difficulties that may arise since these rules and procedures are included in a privately negotiated set of terms at some level of a governance structure." "In the physical world, a signed agreement might be enough to make a legal deal most of the time. But, in the digital space, this is different, especially when it comes to blockchain." "This difference is in how blockchain systems and apps are set up." "The hierarchy should be laid out to have a comprehensive picture of how a blockchain transaction should handle various problems." "To determine whether blockchain governance is successful, we should look at its results" "For this matter, most consortium blockchains should also take an off-chain approach that is more traditional governance by organizations."	"As for auditing the network, our Corda DLT solution provides traceability of the records on the blockchain." "We have an independent Dutch Foundation called The Corda Network Foundation established to oversee the organization" "A non-profit organization with no shareholders but a governing board made up of nine members who were early adopters of the network like B3i and Marco Polo and two members from the R3 network." "The board's goals are to keep the network safe and efficient while also allowing it to expand to its full potential." "That's why participants must make up the Foundation's board of directors and have the authority to vote instead of shareholders." "These directors will serve three-year terms with the primary purpose of guiding the company." "They are also responsible for keeping a close eye on the Network Operator to ensure that it provides dependable and stable service and that its users are satisfied with its work" "Furthermore, they make sure that a network's participation and transaction charges are determined, focusing on maintaining low	"It all began with the concept of a distributed network of linked nodes that could be used to handle any agreement between any parties." "The critical aspect was that these nodes were linked to a worldwide network where parties were aware of their trade partners their identities." "Corda Network is a network of 'nodes' or identities that allows fast, safe, and private transactions using Corda software." "As it currently stands, the network is geared toward commercial usage, and we see a wide variety of sectors joining via pre-formed business networks or groupings of legal organizations with whom they want to deal. The network has features like an identity issuance service in which membership is necessary, a network map, and at least one notary cluster responsible for certifying transactions across the chain." "The parties can automate their different responsibilities after establishing a contractual connection with one another." "In order to join the network, the entity must first construct a node and then receive a Participation Certificate that grants their node permission to the network."	"It provides transparency to the network where each node can audit the chain for themselves"	76

		"For example, if a consortium of European businesses decides to form a governing body, it is logically and likely to settle in Europe instead of Asia." "The board, on the contrary, must include representation from the blockchain consortium and its most important stakeholders." "As for auditing the network, our Corda DLT solution provides traceability of the records on the blockchain."	costs for users, which we call pricing the network." "We created the following governance structure, which we call Corda Contractual Hierarchy (shows picture)." "The structure is what we call a 'self-contained governance' model." "The model's goal is to guarantee that all legal issues have been resolved." "'Self-contained governance' means that there is no need for an outside expert to provide guidance on a blockchain transaction's rules or how to deal with any difficulties that may arise since these rules and procedures are included in a privately negotiated set of terms at some level of a governance structure." "This is crucial because if good governance is lacking, conflicts occur which could have been prevented." "As can be seen, a different hierarchy is at work in this instance." "To determine whether blockchain governance is successful, we should look at its results" "A adequate governance structure should provide intellectual property ownership and license." "Moreover, it should focus on selecting the correct entity, identifying stakeholder	"A non-profit organization with no shareholders but a governing board made up of nine members who were early adopters of the network like B3i and Marco Polo and two members from the R3 network." "After obtaining a Corda Network Participant Certificate, a legal entity becomes a Corda Network Participant and begins using the Corda Network Node." "Corda Network Participants are classified into 'participants' and 'sponsored participants.'" "Participants have legal contracts with R3, whereas sponsored participants are nodes who get access to the network through a participant's agreement." "All Participation Certificate requests will always come via participants, resulting in sponsored participants not seeking certificates directly from R3 because they can get access through sponsored participants who already have access to the network." "Organizations who do not pass R3's sanctions screening will be denied a Participation Certificate and therefore to access the network" "Sponsoring Participants are responsible for adequately guaranteeing and confirming the identification of Sponsored Participants and		

			classifications, representational design, and voting privileges reserved for issues of importance." "On-chain governance like DAOs (decentralized autonomous organizations) are new and have many risks involved, such as mistakes in smart contracts" "For this matter, most consortium blockchains should also take an off-chain approach that is more traditional governance by organizations." "Another factor of successful governance is that all stakeholders should be recognized, and decision-making power should be determined." "The next step is for the organizers to determine how the various stakeholder groups will be represented inside the network and how the board of this network will be organized." "The board, on the contrary, must include representation from the blockchain consortium and its most important stakeholders." "Member's periods of service on the board will typically be the same as those of the board members." "If the board is large enough, and if there are enough stakeholders to give Board decisions credibility, the majority will be determined by the size of the board"	undertaking any due diligence and sanction checks required to ensure that all such businesses comply with the relevant Business Network's tolerance requirements." "However, nodes on the Corda Network may not reject communication coming from other nodes on the Corda Network that are using the routine Corda Protocol, even if they support and utilize expanded versions." "There are two ways to join our network" "Directly is when the node of a direct participant may belong to one or many business networks" "Once the participate is in the network, they will be required to sign a Participant Terms of Use in the onboarding process with R3, pay any outstanding costs for utilizing the network, and seek a Participant Certificate themselves." "Indirectly via business network operator is when a business network operator adds nodes to the network owned by a separate entity." "The board's goals are to keep the network safe and efficient while also allowing it to expand to its full potential." "More specifically, this involves evaluating the network operator to see		

			"Additionally, how many votes each board member casts will be influenced by the structure of the board and the necessity for legality for such choices" "Decisions often need a majority vote of the board's members to modify the board's composition, allocate seats among membership classes, and pass a bill." "Executives are nominated by the board and are in charge of the consortium's daily operations, and the board must determine which officers are necessary." "Finally, The board members may insist on further approval for choices like the approval of the category of members, even if board approval is often utilized for regular project decisions."	whether they're doing good work, deciding on price and scope, and regulations." "It further consists of the network's trust root that serves as a Certificate Authority (CA) that conducts sanctions checks and provides identity certificates to nodes to join; the network's nodes are listed on a map, and the Network Operator or participants themselves can execute the consensus mechanism for nodes to interact over it." "This infrastructure is supported by all nodes, allowing for frictionless transactions between any node in the network." "Furthermore, they make sure that a network's participation and transaction charges are determined, focusing on maintaining low costs for users, which we call pricing the network." "Also, changes to network characteristics and improvements to the system are all approved and communicated with the rest of the network, and the Foundation's structure, voting procedure, standards, and any modifications to the Foundation's governance are done correctly." "From this viewpoint, it becomes evident that each component of the network must consider specific concerns." "For example, the stability,		

				size, and interaction of the users with the network and how key stakeholders are involved in this process." "For example, lots of networks have a variety of nodes like enterprises, service providers, academia, non-profits, and platform users." "Executives are nominated by the board and are in charge of the consortium's daily operations, and the board must determine which officers are necessary." "By restricting the number of Board members from a single organization or set of associated companies, many consortia guarantee that a single entity does not have excessive influence over the consortium." "We have all of the big four companies or actually divisions of them in our network: Deloitte Blockchain, Ernst & Young Blockchain, KPMG International Cooperative, and PwC." "We have all of the big four companies or actually divisions of them in our network: Deloitte Blockchain, Ernst & Young Blockchain, KPMG International Cooperative, and PwC." "It provides transparency to the network where each node can audit the chain for themselves"		

Respondent 4 Gr=94	"That is why we do not do any assurance because we are not selling the solution to our members." "No, we don't. We don't currently. Again, it will depend on the implementation as a Hyperledger. We don't provide any audits like a company. We only offer our open-source code." "Now, I was just in Paris at a conference last week, and there were a couple of people came to us and said we are a blockchain audit company." "And I am sure you heard about a couple of them already, like ChainSecurity and Paladin." "So when people implement it, they can create what they want, and they can either hire one of these audit companies or set it up so that it can be audited. But it's always use case dependent.	"Hyperledger was launched on 9th February 2016 in San Francisco, California. It was founded to advance blockchain technology and to make it mainstream" "Hyperledger is a free and open-source distributed ledger technology developed by the Linux Foundation." "We are often referred to as an IBM blockchain or a private permissioned blockchain, and most of our installations are private" "We have a variety of various blockchains, including Hyperledger Fabric." "However, our market share decreased this year due to a large number of businesses joining Enterprise Ethereum." "We are an open-source organization with five different Hyperledger blockchain projects at the moment: Indy, Iroha, Sawtooth, Besu, and Fabric. Iroha and Sawtooth are both multifunctional blockchains, but a significant portion of both, particularly Iroha, is utilized in central bank experimentation with digital currencies." "I understand the confusion. It was also even confusing for me because often, people think that we are IBM or at least connected with IBM and that we are selling our solution." "Even though we are one of the biggest enterprise blockchains, our team consists of around 11 people."	"The Hyperledger Foundation Charter, as modified from time to time by the Governing Board with the Linux Foundation's approval, applies to all Hyperledger Foundation members, including Associate Members." "Moreover, every member of the Linux Foundation's Board of Directors and the Hyperledger Foundation must follow the policies implemented from time to time by the Linux Foundation's Board of Directors and the Hyperledger Foundation." "Furthermore, non-profits, open-source initiatives, and governmental entities cannot become Associate Members of the Hyperledger Foundation unless authorized by the Governing Board" "Members of an Associate Member get no advantages or rights as a result of their membership in the Hyperledger Foundation, except for the TSC, which the TSC members choose, the Governing Board, Marketing Committee, and any other committees formed by the Governing Board may be represented by a Premier Member representative." "One representative for every 10 General Members may be elected to the Governing Board each year, up to a maximum of two representatives, provided	"Our network also consists of member organizations that are providers of solutions." "R3 is also different because it is a consortium of banks, and they don't like to share data with competitors and therefore need to have some privacy." "So it was basically like a VPN, a virtual private network on a public Internet." "I think we're seeing more of this shift right towards the sort of hybrid network having a private channel on a public network." "Also, like from the academic part of the Hyperledger, I'll be happy to share with you, you know, because I was writing a bit of governance myself, especially about this consortium governance." "And these are all of how these rule sets are defined. We're talking now about some supervisory board or, like the audit nodes there, how these rules are created and developed outside the blockchain."	"Just because blockchain says it is there, it doesn't have to mean it is also physically." "And then I was referring to it, and it's often heard as a sort of like an on-chain and off-chain governance." " Whereas then, and I think that's what you're also looking at, is often called off-chain governance." " And these are all of how these rule sets are defined. We're talking now about some supervisory board or, like the audit nodes there, how these rules are created and developed outside the blockchain."	66

		"To become a member of the Hyperledger Foundation, all Premier and General Members must be current corporate members of The Linux Foundation." "The Hyperledger Foundation Charter, as modified from time to time by the Governing Board with the Linux Foundation's approval, applies to all Hyperledger Foundation members, including Associate Members." "Moreover, every member of the Linux Foundation's Board of Directors and the Hyperledger Foundation must follow the policies implemented from time to time by the Linux Foundation's Board of Directors and the Hyperledger Foundation." "Furthermore, non-profits, open-source initiatives, and governmental entities cannot become Associate Members of the Hyperledger Foundation unless authorized by the Governing Board." "The Governing Board will determine how the election is held. Premier Members, General Members, and Associate Members are eligible to attend general meetings, projects, events, and other similar activities and declare themselves to be Hyperledger Foundation members." "Contributors provide code, documentation, and other technical items to the codebase, wiki, and different Hyperledger outputs."	that at least one General Member representative is always present, regardless of the number of General Members." "The Governing Board will determine how the election is held. Premier Members, General Members, and Associate Members are eligible to attend general meetings, projects, events, and other similar activities and declare themselves to be Hyperledger Foundation members." "The governance structure consists of three components of governance: the Governance Board, the Technical Steering Committee, and the Marketing Committee." "The 'Governance Board' consists of 21 Premier Members, with one representative nominated by each Premier Member, elected General Member members, and a Chair elected by the Technical Steering Committee." "The Governing Board is responsible for approving budgets governing the use of Hyperledger Foundation collected from all sources of income; appointing a Chair of the Hyperledger Foundation to supervise at Governing Board meetings, approve expenditures, and oversee any day-to-day activities; supervising the commercial and marketing operations of the Foundation; and adopting			

		"In addition, The TSC is responsible for choosing a TSC (Technical Steering Committee) Chair, who is also a voting member of the Governing Board and must act as a liaison between the Governing Board and the Hyperledger Foundation's technical leadership." "Lastly, the TSC is responsible for: - Hyperledger Foundation's technical direction; - Approving project proposals under the TSC's approved project lifecycle document; - establishing cross-project working groups to address technical difficulties and opportunities; - exchanging information with other organizations about relevant technological issues; - representing other standards groups by nominating representatives; and - coordinating with the Hyperledger Foundation's Advisory Board. "Indeed, Corda was created by R3, a banking consortium." "So at its core, R3 started growing out of different because a consortium of companies began it." "When I did my Ph.D. in 2017-18, the consortium topic started to take off. Then people try to categorize it nicely into the consortium classes business, technology, or dual-focused. Afterward, everything got a little bit mixed up and complicated. So this taxonomy is not developed at all." "But that's nature; however,	and upholding the Hyperledger Foundation's rules and regulations, such as its Code of Conduct, trademark policy, co-branding policy, and co-development The 'Technical Steering Committee' comprises fifteen Contributors or Maintainers elected by Active Contributors who have a weekly meeting on Thursday which can be checked in our community calendar because it's open to everybody." "In addition, The TSC is responsible for choosing a TSC (Technical Steering Committee) Chair, who is also a voting member of the Governing Board and must act as a liaison between the Governing Board and the Hyperledger Foundation's technical leadership." "Lastly, the TSC is responsible for: - Hyperledger Foundation's technical direction; - Approving project proposals under the TSC's approved project lifecycle document; - establishing cross-project working groups to address technical difficulties and opportunities; - exchanging information with other organizations about relevant technological issues; - representing other standards groups by nominating representatives; and - coordinating with the Hyperledger Foundation's Advisory Board." "The 'Marketing Committee'			

		blockchain is something that is not fixed at all." "R3 is also different because it is a consortium of banks, and they don't like to share data with competitors and therefore need to have some privacy." "However, we are seeing more shift towards having a private channel on a public blockchain. EY was one of the pioneers of that. I believe it was called the Nightfall protocol, which meant that there was a private channel on the public blockchain or public Ethereum." "I think it's always good to get some order into things, and I would say that TradeLens is a Business-Focused consortium." "But again, if you're thinking about, for example, Hyperledger, it is not so fixed as always thought "You can say that the blockchain says it's in Burkina Faso right now" "Just because blockchain says it is there, it doesn't have to mean it is also physically." "I also thought previously that this was the case when I joined initially. Hyperledger Fabric, Corda, and Enterprise Ethereum are the most used enterprise blockchains." "IBM takes the source code, reuses it, and develops their blockchain called IBM blockchain." "Walmart, for example, has food traceability. These are all	comprises one voting representative from each Premier Member, one or more non-voting Maintainers nominated by the TSC, and one or more non-voting representatives." "Last but not least, the Marketing Committee is responsible for the formulation, creation, and execution of the Governing Board's marketing strategy." "Also, like from the academic part of the Hyperledger, I'll be happy to share with you, you know, because I was writing a bit of governance myself, especially about this consortium governance." "And then I was referring to it, and it's often heard as a sort of like an on-chain and off-chain governance." "Whereas then, and I think that's what you're also looking at, is often called off-chain governance." "And these are all of how these rule sets are defined. We're talking now about some supervisory board or, like the audit nodes there, how these rules are created and developed outside the blockchain."			

		built on IBM blockchain and not Hyperledger." "Also, like from the academic part of the Hyperledger, I'll be happy to share with you, you know, because I was writing a bit of governance myself, especially about this consortium governance." "So on-chain is whatever can be programmed into the blockchain itself." "You have these programmable rules, and then you make them follow. You often hear that blockchain is immutable, but they're talking about bitcoin's blockchain, not really about enterprise blockchain, where you can have two or three nodes." "And these are all of how these rule sets are defined. We're talking now about some supervisory board or, like the audit nodes there, how these rules are created and developed outside the blockchain." "Now, I was just in Paris at a conference last week, and there were a couple of people came to us and said we are a blockchain audit company"				

Respondent 5 Gr=96	" We've built this functionality based on how the insurance companies or brokers, or reinsurers want to use this functionality to satisfy their audit requirements" "The part that I was going to show you is in terms of the audit trail; this is the part that I was thinking might be of interest, which is where you can go into the contract." "With all these online interactions, you can click into the audit trail." "And the audit trail screen provides a summary of all the changes between the current and the previous version, and a new entry is created every time the contract is shared, allowing the user to trace all the changes since the beginning of the negotiation." "They would have whatever their existing practices with auditability of various different reinsurance contracts that are placed." "Once again, from an auditability perspective, you know, firstly, you can make sure that the person with the authorization is given access to the application, and you can set their limits to make sure that they are registered as an authorized signatory within the blockchain application." "You're about to enter into a legally binding transaction by clicking this box and then going back to the audit trail." "This would be able to show you precisely who signed and when they've signed, and the end pulls end-to-end auditability goes in through all stages of the value chain."	"I will just quickly show a screen. I won't go through this in detail. I got two slides on the history of B3i. We were founded initially as a consortium, and it was born out of a project that we had with some of our shareholders, and we focused on a reinsurance use case." "One of the network parts is a segregated network within the underlying called Corda network." "Corda is broader than the B3i network." "When you log in to the blockchain application, you log in via a node. It's just a technical term for the log-in section. And customers have got a choice. They can develop the technical setup on-premise in their own IT infrastructure, or they can have B3i node as a Service (NaaS), which is where we have a subscription model where you can subscribe to our node as a service model." "We've developed a platform because we recognize that some insurance-specific functionality is needed to support our blockchain-based applications." "At B3i, we've built this blockchain-based reinsurance application." "Within this is the blockchain-based application, you've got the risk details and the preliminary, which is basically where we start to structure the treaty, and it will go into layers and sections so that many risks will be broken down into various	"And then, in terms of the governance of the network, as I said, we do a quick check for the initial onboarding."	"I will just quickly show a screen. I won't go through this in detail. I got two slides on the history of B3i. We were founded initially as a consortium, and it was born out of a project that we had with some of our shareholders, and we focused on a reinsurance use case." "We did what we call a hackathon, where several participants were invited to play the role of the various parties that would be part of the reinsurance network." "We'd follow all of our protocols regarding the onboarding and the safekeeping of certificates and things like that to access the network." "That then enables us to do the onboarding to the business network." "And in the once they are a member of the business network, we've then got a legal agreement, which is all the terms and conditions and terms of being a member, being a member of the business network." "B3i is a network consisting of our shareholders, which we've developed three core parts of our product and service proposition." "One of the network parts is a segregated network within the underlying called Corda network." "Corda is broader than the	0	30

		layers and sections." "Once again, from an auditability perspective, you know, firstly, you can make sure that the person with the authorization is given access to the application, and you can set their limits to make sure that they are registered as an authorized signatory within the blockchain application."		B3i network." "It's like encompasses all aspects of financial services. You've got banks, insurance companies, and other financial services providers at B3i." "We've got a sub-network within their network that focuses specifically on insurance companies, brokers, and reinsurers." "It's called the B3i Business Network." "We do the KYC and onboarding to that network." "And to be able to access the network, you need to have what we call a node."		

Respondent 6 Gr=83	0	"And to be able to access the network, you need to have what we call a node." "That's why I believe private blockchain or small consortium blockchains will disappear and are not the future is because the whole point is that you can trust the network without trusting the other party." "So those in this group agree on their way to do it. So if you have, for example, the Microsoft blockchain for Xbox and then you have Nintendo, that comes to it, right? Well. Microsoft owns one of the two companies, by default, owns at least 50% of the nodes since the two companies own 100% of the nodes." "Because it's part of the Smart Contracts concept. But technically, it's not purely data that comes from the blockchain." "Well, I don't know all the blockchains in the world." "So maybe there's a way to block a private key from doing transactions on the blockchain in some systems." "It would take off some of the power of the blockchain itself because if you could have a validation on the blockchain of who can write or sign the transaction." "Because if you have a protocol like Bitcoin where you have 10 minutes between blocks," "It's not a significant KPI that you have this replication that	0	"So obviously, in a consortium, you have some grasp on where the data is located since it's the consortium that determines where the nodes will be located." "But if you have a consortium between multiple companies, you need to make sure that all the companies comply with all the regulations that the companies need that make sense." "For example, if you have a multinational that operates in Germany and then another company in the consortium that operates in the US, you must comply with both regulations." "You have to ensure that if you have more than one company in the consortium, that is the whole point of a consortium. Ensure that all the people acting within that sort of internal, semi-private network are." "But, for example, we could say that the network is not allowed to connect to nodes outside the IP address range to make sure." "For example, all the network nodes are located in the approved regions." "But if the other party is the network, then how do you trust it? So I would keep it, but it only works in, as you mentioned, a vast number of participants. I would say maybe ten or more or	"Okay. So when you say off-chain, it refers to the infrastructure and how the infrastructure communicates with each other. Like we're talking about the nodes?" "Because you're focusing off the chain, you could also have come off-chain preventive controls." "It depends on whether that permission, that identification of the different nodes and the way the protocol communicates, the information you consider on-chain or off-chain." "As for control 20, that's off-chain for sure. That is the Decentralization or enforcement of consensus protocol. The one is off-chain. I mean, that's part more of a jurisdictional jurisdiction. I mean, you're not talking about automation or anything. You're talking about whether people are able or not to do some inside trading." "Like you could have something that is off-chain in terms of preventive control." "However, some parts of the consensus can be unchained, too." "For example, a node is off-chain if it's physical assets" "You talk about nodes that are off-chain." "Yeah, you could, but I would still put it classified as	41

		happens instantly, whereas you have a blockchain where you know." "The monitoring is not part of the blockchain" "Appropriateness of KYC, this is the number one issue we had when those Bitcoin and Ethereum we're using as transactions is how do we know who's behind it." "There's no way for you to say to the blockchain, stop accepting this private key"		something like that, you see." "So those in this group agree on their way to do it. So if you have, for example, the Microsoft blockchain for Xbox and then you have Nintendo, that comes to it, right? Well. Microsoft owns one of the two companies, by default, owns at least 50% of the nodes since the two companies own 100% of the nodes." "Like, a node from Russia pops up in the network. You say, do not connect to it." "We're talking about networking, but we're talking about networking in terms of package size, which is directly correlated to. How your network scales, which is directly correlated to." "Protect the network from access." "Right. And that would the way you would prevent this is very similar to how you would prevent a node from connecting from Russia, for example. You would have a whitelist of known nodes within the network." "The only thing with the whitelist that I can see is that because of consensus, you're not in a purely private blockchain, so you still potentially have people that get appended to the network without contacting all the participants." "And so you would have to	off-chain to me." "To your protocol of the chain' "The information is nearly instant, and that's a significant KPI. So to me, that's still off-chain.' "But yeah, for me, it's still off-chain because it's." "But how do you link a public key and the physical person or entity behind it? That's super important." "So that whole system that I just described for me is entirely off-chain."	

				update that whitelist all the time, you see. If you have a new company that joins that consortium, they would need to inform all the other companies that this company has entered and has added a new node or new nodes"		

Respondent 7 Gr=25	"What goes into this database so you can audit it?" "This is looking at it from an audit view. I'm not sure if you're aware of the IPE (Information produced by the entity)" "And that cannot be audited just exclusively with analytics or these things."	"Several years ago, I also did my master thesis on blockchain, which revolved around blockchain applications." "What do you mean precisely with access in this case? So just generally, what is the idea of access here? Do you mean only the parties involved in this consortium blockchain have access and/or employee user or client users of the individual firm node that can access the data?" "Indeed, in the end, you have several options going into this one blockchain or putting data into it." "I mean, in the end, it's a database." "What goes into this database so you can audit it?" "In the end, the intended and relevant information should only end up in the database, I guess, in the case of payments."	0	"But, depending on the setup of this consortium, etc., it might need to be adjusted" "What do you mean precisely with access in this case? So just generally, what is the idea of access here? Do you mean only the parties involved in this consortium blockchain have access and/or employee user or client users of the individual firm node that can access the data?" "And then it could also be that the participants of this consortium are changing, that they have some new companies coming in and are not part of it or are temporarily part of it. And in that case, it's probably the same: it would need to be adjusted."	"Who has this off-chain database?" "It's about keeping today's employees, for example, who come and go out of the company. That's probably, in your case, different kinds of companies, types of companies. And they all have their own off-chain, which could be an SAP or something"	14

Respondent 8 Gr=39	"Control 3 is essential, as you want to have a responsible entity that takes responsibility for audit procedures or is accountable in case of conflict." "That's the reason why we auditors have to audit the blockchain." "Those controls are audit & monitoring related. Which is important to review periodically. They look good to me."	"As for the second control, do you think about the blockchain as a system or a system where you can put something in it. In order words, you consider this control if you consider the blockchain an IT system, operating system, or database." "Control 6 is, I would guess, the responsibility of the blockchain provider?" "So in countries such as Estonia and Salvador, blockchain cryptocurrencies like Bitcoin and Ethereum were regulated. So yeah, you can compute it because, first of all, before implementing the blockchain, you have to be sure that that in that country is applicable." "You have the transparency and are sure that those transactions were made on the blockchain." "But not all the transactions will be traceable on the blockchain, just like the last one, the balance sheet." "Now because, for example, on the blockchain, on the off-chain where you are, that would be very like." "That's the reason why we auditors have to audit the blockchain." "We did, for example, because, you know, there is a conflict between the blockchain and the European Commission." "The Blockchain Foundation commented from their side that the data you put in the	0	"Nodes on the Lightning Network. Download the software and create change channels between themselves and another node while users have a wallet that sends or receive payments to the network on the network."	"So, in that case, some of our transactions are not traceable if they were off-chain." "Now because, for example, on the blockchain, on the off-chain where you are, that would be very like." "There are also many videos on YouTube about Lightning Network, the application, and how to change." "Nodes on the Lightning Network. Download the software and create change channels between themselves and another node while users have a wallet that sends or receive payments to the network on the network." "There are systems like Lightning that requires a multi-signature address."	22

		blockchain is not necessarily personal data because you can use the hash to put your data in the blockchain." "For example, we have four nodes. It's enough to corrupt three if they would attack the blockchain." "It is just that the end transaction will be put on the blockchain, for example, and not all the transactions." "At the end of the exchange or business, the final balance sheet is sent on the blockchain, but not the intimidating one." "For example, I have one I have to send to you. For example, 0.5. So you will have +0.5, and I will have -0.5. Let's say the second transaction. You send me 0.2. As I only use money at the end of the month. Let's say this is our last transaction. This is the balance sheet. This balance sheet is like any cell will be uploaded, or we will be updated every time we have a transaction. The last transaction would be put on the blockchain. So, in the end, you will have on the blockchain that I sent you 0.3, but you will not have these intermediary transactions."				

Respondent 9 Gr=49	"When you audit a blockchain like this, the first step you likely take is scoping or a process?" "The scoping, I think, is part of how you approach the audit from the other perspective." "Think, okay, this client has a particular question. What can we do to help them?" "So then you go and identify, for example, your approach, the authenticity, and the auditors, together with the client, arrive at the scoping." "So it has to be clear what we're talking about, who is performing the process, and the frequency with which it's performed."	"But I think blockchain has probably a different story because their issue is that the risk is that you forget certain areas." "I have to say, I'm not very familiar with the most critical risks for blockchain because it's not my field activity per se." "Blockchain, I think that's a very new area. Normally you identify the most critical risks."	"Because when you dissect an issue, for example, in a network governance area."	"Because when you dissect an issue, for example, in a network governance area" "For a network benefit, for example." "Yeah. I think I think maybe the network ones can be combined into one." "You think about combining like this, you have four separate controls for one or two, maybe for the network ones." "You could also think of something like that where you don't have all these separate controls, but it's more the combination of controls that supports the network."	0	14
Respondent 10 Gr=9	"Indeed, actually, for every audit, it doesn't matter if it's a financial IT operation or cyber audit or something. You always have preventive, detective, and corrective controls."	0	0	0	0	1
Respondent 11 Gr=42	"There is also a standard setup that states will control, providing reasonable assurance that some control objectives seem to be a little more controlled." "So our controls provide reasonable assurance that." "We often use a sample-based approach to be able to come up with "reasonable assurance." So no "full assurance" or "100 percent assurance" that those changes have been approved."	0	0	"Member skills are available and in the network."	0	4

Respondent 12 Gr=20	"That's more for SOCR. So as auditors, what we're trying to do is we're trying to look at risks and see what we can do to mitigate those risks" "And that's what we look at. Of course, we have improvements"	"And what's also important to mention then is that if you look at risk can be applicable for all sorts of blockchain areas or even for all the blockchains in general." "So, during my own thesis, I wrote about blockchain and the risk controls arising from blockchain." "So when we look at a consortium blockchain, right. It's a very interesting type of blockchain that you also, somewhere in your thesis, built like a little bridge to, let's say, a public blockchain or a strictly private blockchain and, well, to dive a little bit deeper in." "That's because the blockchain is not all the same as a public blockchain, for instance, so the results from the framework should not be interpreted as such." "I thought blockchain was just blockchain. But yeah, there is so much there are so many differences in all of those sorts of blockchain."	"That's something to do with network effects of governance"	"That's something to do with network effects of governance,"	0	9
Totals	40	98	51	78	27	294

Appendix E: NOREA Congress


NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS
30
Make IT Happen
Het break-out deel van het programma bevat onderstaande areas
Vitale Sectoren
In deze area betreden key players uit vitale sectoren de boksring om met elkaar uit te vechten hoe de digitale weerbaarheid in hun sector verbeterd kan worden.
Keeping us safe: onze veiligheid
• Politie / Defensie
• Port of Rotterdam
• Onderzoeksraad vd veiligheid
• Universiteit Tilburg
De hardware van Nederland; onze digitale infrastructuur
• Agentschap Telecom
• KPN
• DINL
De financiële sector
• ABN AMRO
• Nationale Nederlanden
• Ohpen
• Autoriteit Financiële Markten
• De Nederlandsche Bank
De overheid
• CIO Rijk
• Sociale Verzekeringsbank
• Auditdienst Rijk
• NCSC
Dilemma's en disrupties
Hete hangijzers voor de digitale weerbaarheid van onze samenleving, en wat we kunnen doen om deze te verbeteren.
Nieuwe vormen van cybercrime
Wat komt er na DDOS en ransomware? Wat zijn de trends en hoe kun je je er tegen wapenen?
Quantum computing als disruptor
Wat is quantum computing en wat gaat dit in ons digitale landschap veranderen? Wat moeten we nu al doen?
Omgaan met cyberaanvallen
Wat moet je doen als je gehackt wordt? Welke scenario's zijn er? Wat zijn de do's en don' ts?
Gebruik en misbruik van algoritmes
Modellen en algoritmes worden steeds slimmer. Maar er gaat ook veel fout. Waar ligt de grens?
De risico's van crypto's
Hoe kunnen crypto's betrouwbaar ingezet worden?
Digitaal boeven vangen
Ook onze handhavers worden steeds digitaler. Hoe gaan zij te werk?
Het IT Audit beroep
Het IT audit beroep is volop in beweging. In deze area belichten we nieuwe ontwikkelingen en creëren we mogelijkheden om met elkaar in gesprek te gaan.
De IT Audit Verklaring
Een initiatief van NOREA om het maatschappelijk verkeer meer zekerheid te geven over de IT van organisaties. Wat is het precies en hoe werkt het?
TED talks NOREA kennisgroepen
Korte presentaties door NOREA kennisgroepen over bevorderen van digitale weerbaarheid op hun kennisgebied.
ZZP'ers united
Een bijeenkomst voor en door ZZP'ers op gebied van IT Audit.
Potentie van de RE als professional
Een RE-titel is vaak de start van een boeiende carrière. Kom luisteren naar aantal van deze verhalen.
Young profs en studenten
Een fysieke clubhouse sessie over het IT Audit beroep en wat dit aan Young Profs te bieden heeft.
Mogelijk gemaakt door:
EY
Building a better working world
Auditdienst Rijk
Ministerie van Financiën
BDO
pwc
bakertilly
KPMG


NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS
30
Make IT Happen
1 1 1 1 0
De volgende organisaties en personen zullen bijdragen aan het congrestival:
Organisatie | Persoon | Functie
ABN AMRO | Martijn Dekker | CISO
Agentschap Telecom | Angeline van Dijk | Bestuurder
Auditdienst Rijk | Adri Kerkvliet | Algemeen directeur
Autoriteit Financiële Markten | Tom van de Ven | Manager Operational & IT Risk
De Nederlandsche Bank | Nicole Stolk | Directielid
DINL | Michiel Steltman | Managing Director
ECB | Evelien Witlox | Program Director Digital Euro
EY | Rudrani Djwalapersad | Partner
Eye Security | Job Kuijpers | CEO
Financieel Expertise Centrum | Iris Sluiter | Head of FEC-partnership
FIOD | Team digitale expertise | Teamleider
ING | Adil Acun | Lead Quantum Engineer
Inspectie Leefomgeving en Tranport | Rene Putters | Afdelingshoofd
KPN | Paul Slootmaker | CISO
NN Group | Rob Visser | Group CIO
NEN | Ruud Kerssens | Expert member AI
Ohpen | Matthijs Aler | CEO
Onderzoeksraad vd Veiligheid | Marjolein Baart | Onderzoeker
Politie | Team digitale expertise | Teamleider
Port of Rotterdam | Marijn van Schoote | CISO
PWC | Mona de Boer | Partner
Sociale Verzekeringsbank | Britt van den Berg | CIO
TNO | Thijs Laarhoven | Onderzoeker
Universiteit Tilburg | Kenny Meesters | Onderzoeker
Simon Lelieveldt | Regulatory and Compliance Consultant
En tal van overige organisaties
Mogelijk gemaakt door:
EY
Building a better working world
Auditdienst Rijk
Ministerie van Financiën
BDO
pwc
bakertilly
KPMG