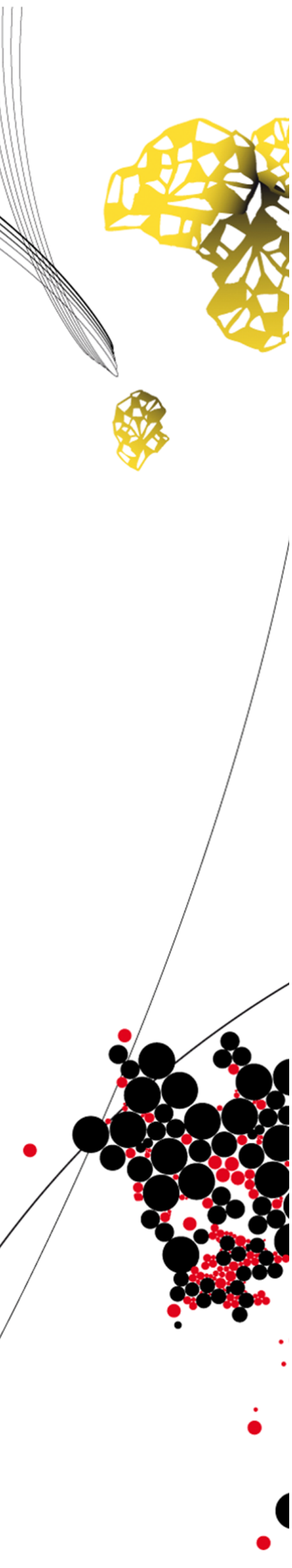

UNIVERSITY OF TWENTE.

Faculty of Electrical Engineering, Mathematics and Computer Science

Creating an IT Risk Maturity Model for Distributed Ledger Applications

Jaap Vermeij

M.Sc. Thesis

14 December 2018

Business Information Technology
IT Management and Innovation

Supervisors:
Dr.ir J. M. Moonen
Dr. L. Ferreira Pires
(University of Twente)

M.Sc. M. Schäfer
(Robert Bosch GmbH)

Acknowledgements

During this research I have been supported by many people which have helped me succeed. There are a number of people which I would like to thank in particular for their contributing to this research, to my development or to my overall well-being.

I would like to thank everyone within the CI/DAA1 department within Bosch and especially Michael Schäfer in supporting me during the course of writing my thesis. Within the department I got all the freedom to shape my research in the way I wanted and was supported at moments where I needed more guidance.

Hans and Luis have always had their metaphorical door open, even though I was out of the country and we only sat together in person on a few occasions. The collaboration from a distance worked out great and I would like to thank both for their guidance during our effective Skype meetings.

Throughout the course of the research I've had contact with many people from different companies which have helped me out in the research by joining the Delphi panel or assisting me in any other way. Thank you to all of you since without you joining the research, it would not have been possible to complete it in its current form.

Finally I would like to thank my family and my girlfriend who have helped to support me mentally and put in quite some hours reviewing all of my work.

Summary

Distributed ledger technology (DLT) has been gaining in popularity for businesses and academics alike in the previous years. The promise of DLT is that it ensures shared control over data without a central party to control these data. With DLT, businesses no longer need to base their trust in the integrity of the data on this central party since DLT systems can potentially guarantee this integrity. Distributed ledger technology is still a young technology and there are only a limited number of organization which are using applications with DLT. One of the reasons that it's not widely used yet is due to the risks involved with the technology. Identifying risks specific to DLT is difficult with current risk assessment models. This research proposes a new IT Risk DLT Application Maturity Model which can be used by businesses to asses risks of DLT and enhance their development processes.

In this research, a multi-method approach was applied to develop a maturity model. We started by identifying IT risks of DLT applications through a literature study. The risks identified in literature were presented to a panel of 15 experts from various companies and academic institutions in a two round Delphi study. The panel proposed a large number of additional risks that have been consolidated into a total of 48 risks divided over 5 risk areas and 14 sub-risk areas. We found that there were many risks that are not mentioned in literature which are considered important to businesses. The combination of both fields provide valuable insights for both academics and practice.

The risks that were collected were further verified within five different case studies. Within these case studies, it was found that the identified risks are not generalizable to every DLT application. There are aspects, such as DLT performance, which differ per use case. In order to define these restrictions of the model, criteria have been drafted which the use case should adhere to before the maturity model can be applied.

For each of the 14 risk areas, five maturity level descriptions were defined based on the definitions of the CMMI levels in combination with the identified risks. These level descriptions were checked once more by a panel of experts through a survey. In this survey, we found that a number of areas, such as the Data Management area and the Endpoint Security area, are still in discord. Not all experts agree with the descriptions, but have given feedback on how to improve them. The feedback has been incorporated in the final level descriptions.

The created maturity model can be applied to a DLT application through a number of drafted assessment questions based on the level descriptions for each level. The results of the assessment are visualized through a dashboard to improve the comprehensibility of the results and to quickly identify possible areas of improvement for the applications. Both the assessment questions and the dashboard have been verified with one of the case studies used earlier in the research.

The created IT Risk DLT Application Maturity Model and the collection of IT risks are the most important contributions of this research. The model includes a number of risk areas which can be improved upon in future research. The combination of academics and practice within this research allowed us to create a comprehensive list of IT Risks for DLT applications which can be used both in academics and in practice as a basis for future research.

Contents

List of Figures

List of Tables

Abbreviations

AML	Anti Money Laundering
BMM	Blockchain Maturity Model
CPO	Charge Point Operator
DAG	Directed Acyclic Graph
DLT	Distributed Ledger Technology
ERM	Enterprise Risk Management
EV	Electric Vehicle
GDPR	General Data Protection Regulation
IoT	Internet of Things
IT CMF	IT Capability Maturity Framework
KYC	Know Your Customer
MSP	Mobility Service Provider
MVP	Minimal Viable Product
PoC	Proof of Concept
PoS	Proof of Stake
PoW	Proof of Work
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RMM	Risk Maturity Model

Part I

Spark

Chapter 1

Introduction

Distributed Ledger Technology (DLT) has been gaining popularity in the previous years. Many companies are looking for opportunities to use DLT within their business but there are not many instances where a company moves onto using a DLT application in their regular business processes. Often times after a proof of concept is created the decision is made to not further develop the application since DLT is simply not yet mature enough to perform a vital role within the company. There is currently no method to easily analyze a DLT application that gives an overview of its associated technology and business risks.

The promise of DLT is that it enables shared control over data without a central party to control these data (Hileman & Rauchs, 2017). With DLT, businesses no longer need to base their trust in the integrity of the data on this central party since DLT systems can potentially guarantee this integrity. This opens up new opportunities for businesses for collaborations where previously no central trusted party was available. However, it is still proving difficult to find these new uses and integrate them within their organization. Start-ups have sprouted up around new and improved applications of the technology, and research and development departments at larger enterprises are creating proof of concept applications to be used within their organization.

Bosch is currently in the process of identifying use cases and producing proof of concept applications using distributed ledger technology. Working together with a multitude of partners in different consortia they are producing use cases mainly in the field of IoT and mobility. One of the strategic objective of Bosch is to become an IoT company with many of it's products being interconnected. This idea of an IoT company is leaking through all the different industries in which Bosch is active, from connected industry to smart homes and connected mobility, to only name a few. Simply connecting devices to the Internet is not enough to create an effective IoT network, devices need to be properly secured and methods to manage the devices should be set up. DLT can help to support this network of secured inter-connected devices and create trusted data connections between IoT devices from various organizations.

Distributed ledger technology is a young technology and there are only a limited number of organization which are using applications with DLT. Some organizations have introduced applications using DLT but each application has limitations, such as scalability, security, a centralized governance and others. Popular DLT networks such as Ethereum and Blockchain are not optimized to run together with IoT devices since they require too much power, storage or require the device to be online all the time.

Identifying the limitations and risks of the created applictions can often prove difficult for managers since there is no reference system to compare them to. Existing IT risk assessment frameworks are not suitable for DLT applications since they lack the ability to easily identify DLT related risks such as

the immutability of data and shared governance issues.

Maturity models are often used in larger companies as an informed approach to continuous improvement or as a means of benchmarking and self-assessment. These models often look at larger processes such as the development process of an application, but they can also be applied to assess the maturity of processes surrounding a specific technology. This type of object-specific models can serve as a developmental aid in organizations wanting to develop or implement DLT applications. Using maturity models to assess DLT applications offers managers a structure they are familiar with and it can show different types of risks in a common format.

This thesis will focus on evaluating current methods of IT risk identification using maturity models. After this, a new maturity model is presented which focuses on evaluating the IT risks of DLT applications in connection with IoT. This model is verified through a number of case studies evaluating proof of concept applications.

1.1 Organization Background

This research is being carried out with the cooperation of Robert Bosch GmbH. Bosch is a multinational engineering and electronics company with over 400.000 employees spread out over 60 countries. The company is headquartered in Gerlingen, Germany, close to Stuttgart where it was founded in 1886. In 2017 they had 78.1 billion euros in sales with their mobility solutions business sector producing 61 percent of the sales. Other business sectors they are active in are industrial technology, energy, building technology and consumer goods.

Research and development is a key focus of the company which is always looking to expand and improve their product range. Their objective is to develop innovative, useful, and exciting products and solutions to enhance quality of life. They have around 59,000 researchers and developers working on research at 120 location worldwide. In the past six years they have invested around 27 billion euros in research and development.

1.1.1 Central IT - Advanced Development

Central IT (CI) at Bosch consists of about 5000 employees of which most are located in Feuerbach, Germany, again close to Stuttgart. The Advanced Development department within CI focuses on analyzing IT trends and supporting the operative business units in the pre-development phase. The department is consulting other business units, scouting new technologies, prototyping and creating contacts with universities and other technology leaders. It aims to be the connection between the Corporate Research (CR) division and CI. The department is spread out over multiple locations; Feuerbach, Palo Alto, Pittsburg and Singapore. Within the departments these departments there are teams focusing on different emerging IT technologies ranging from AI to Edge computing.

Within the CI Advanced Development department there is also a focus on Distributed Ledger Technology. The department focuses mostly on the initial generation of business cases and proof of concept development. When a proof of concept (PoC) is deemed to have sufficient potential they are further developed within a different department. The initial risk assessment of these PoCs is not a main focus during this initial phase, but it becomes important when assessing the possibilities for further development.

1.2 Research Goal

The goal of this research is to create a method to evaluate risks of DLT applications to be used by organizations within their development process. This method should help to identify risks and show in what aspects an application can be improved to reduce these risks. Currently, much of the development of DLT applications does not take risks into account in early development since they are either not well known or difficult to evaluate.

This research aims to create a systematic means to evaluate the risks and rate an application based on standardized levels. These standardized levels will form a maturity model which is easily understood by organizations already familiar with maturity modeling. The model will look specifically into risks of the combined usage of IoT and DLT while also being applicable to DLT applications in general. Applying DLT to the IoT presents an interesting opportunity but the are currently still many risks involved in applications harnassing both technologies. The created maturity model can be used for risk assurance of DLT related projects. This can be useful in a multitude of different stages of DLT application development.

1.2.1 Research Questions

In order to achieve our research goal, the following main research question has been defined:

> **Research Question:** *What constitutes a usable maturity model for IT risk assessment of distributed ledger applications in connection with the Internet of Things?*

In order to answer the main research question we have defined a number of sub questions which help guide the research to the answer.

> **Sub Question 1:** What is Distributed Ledger Technology in connection with the Internet of Things?
>
> **Sub Question 2:** What maturity models are currently available to evaluate IT risk maturity of software applications?
>
> **Sub Question 3:** What is the state of the art of maturity models with respect to risks of DLT applications in the IoT domain?
>
> **Sub Question 4:** What are the IT risks and corresponding risk domains for DLT applications in general and specific to IoT?
>
> **Sub Question 5:** How can the maturity levels be defined for each risk domain?
>
> **Sub Question 6:** How can the IT risk maturity of a DLT application be assessed using the created model?

1.3 Research Methodology

In order to create a method to evaluate the risks of DLT applications a maturity model is designed. This type of model is chosen because it is well known within many organizations and can provide a good overview of risks and how well these risks are mitigated.

In the field of information systems many maturity models have been created but they are often criticized for their lack of empirical foundations (De Bruin et al., 2005). To counter this criticism, a number of prominent researchers have proposed research methodologies for creating empirically grounded maturity models (Becker, Knackstedt, & Pöppelbuß, 2009; De Bruin et al., 2005; Mettler, Rohner, &

Winter, 2010). During our research, the design science methodology for maturity models as proposed by Mettler (2011) is followed. He has compared and combined elements from the mentioned research methodologies with his expertise of creating maturity models to create a methodology which includes essential decision parameters from both a developers and a users perspective.

During this research the following four phases of the development cycle are followed:

1. Define scope
2. Design model
3. Evaluate design
4. Reflect evolution

For each of these phases, Mettler (2011) has created decision parameters to help guide the development of the maturity model. The decision parameters for each of the phases are shown in table 1.1.

Before the development cycle starts, the need for a model is established and a review on existing maturity models is completed. An evaluation will be performed to identify if there is a need for a new or adapted maturity model and the first phase of the development cycle is started by defining the scope of the model.

The second phase is focused on designing the model. In this research this phase is divided up into a number of different parts in order to build up the model. The first elements of the model are gathered through a literature review and a two round Delphi study with industry experts. These steps ensure that risks from both literature and practice are covered in the model. The collected risks are further evaluated through a number of case studies. After gathering all the information about the risks maturity levels are created that represent the identified risks.

The third phase, evaluating the design, is done by presenting the design to the the experts which helped to identify the risks in the Delphi study. Furthermore the created model is applied to one of the case studies which has been researched to evaluate its design.

After a final model is presented, the fourth and last phase is the 'reflect evolution phase'. Here, the evolution of the model will be further investigated since the topic of Distributed Ledger Technology is far from mature and changes may take place in the definition of maturity in the field. A guideline should be in place to adapt the model to the changing environment.

Table 1.1: Decision parameters per design phase

1. Define scope	*2. Design model*	*3. Evaluate design*	*4. Reflect evolution*
Focus/breadth	Maturity definition	Subject of evaluation	Subject of change
Level of analysis/depth	Goal function	Time-frame	Frequency
Novelty	Design process	Evaluation method	Structure of change
Audience	Design product		
Dissemination	Application method		
	Respondents		

1.4 Structure of the Thesis

This thesis will follow the development cycle as defined by (Mettler, 2011). The structure of this thesis is build around the different phases of this development cycle. Figure 1.1 illustrates the organization of this research mapped onto the development cycle.

Chapter 2 will define the various concepts relevant to this research and present the state of the art for each topic. At first, the basic concepts behind Distributed Ledger Technology are explained. Second, the concept of Internet of Things will be explained. Third and last, IT risks are defined and the basic concepts behind maturity models are explained.

Chapters 4, 5, 6 and 7 include the design phase of the model. In chapter 4 the risks of DLT as described by literature are collected through a literature study. Chapter 5 gathers additional risks from field experts through a Delphi study. The collected risks are evaluated with a number of case studies in chapter 6. Chapter 7 includes the design of the maturity model with level descriptions based on the identified risks.

Chapter 8 evaluates the created maturity model using a survey and presents a number of assessment questions accompanied by a dashboard to visualize the model. Finally, in chapter 9 the results of this research will be discussed and directions for future research are proposed.

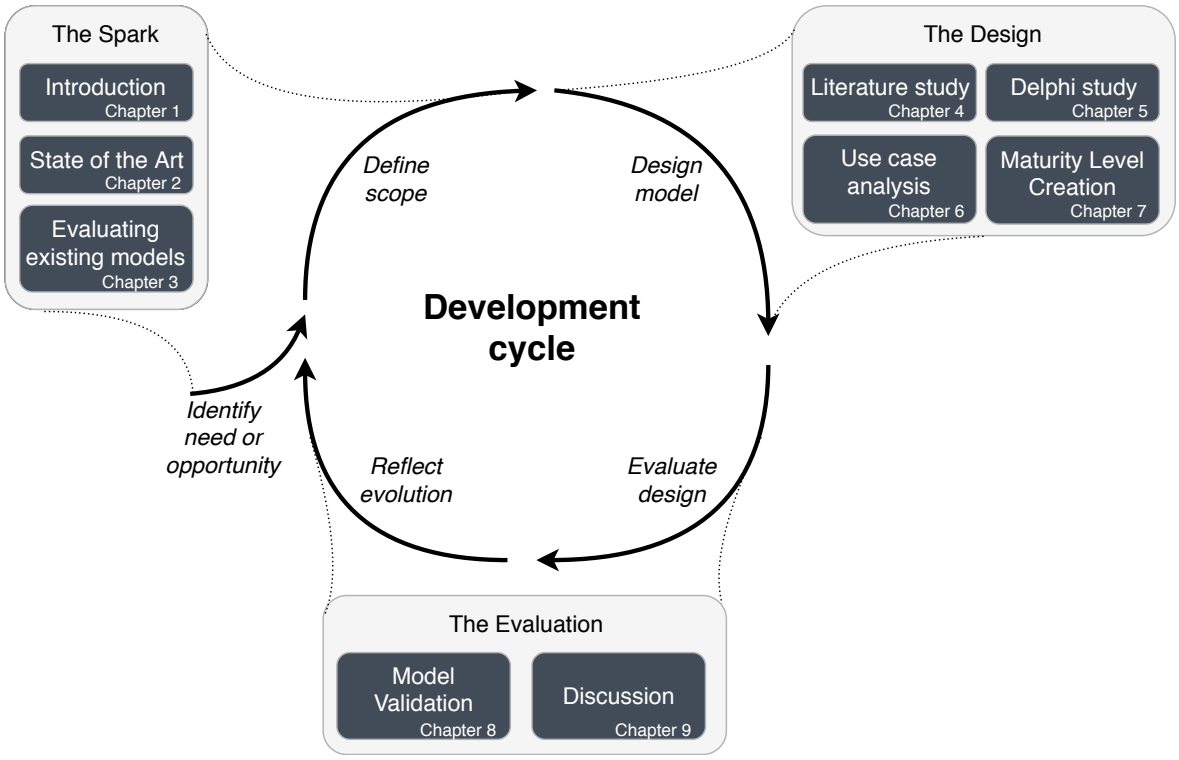

Figure 1.1: Overview of different chapters in this thesis

Chapter 2

State of the Art

This research touches upon a number of topics, some already well established and some which are still developing. This chapter will introduce the different topics on which this research is built and present the state of the art for each topic. First, an introduction to the focus of this research, Distributed Ledger Technology, is given. Second, the Internet of Things is explained together with its close connection to Distributed Ledger Technology. Third, maturity models and their connection with DLT is presented.

2.1 Distributed Ledger Technology

In order to explain what DLT is and how it works, we first have to establish a definition of DLT. The definition of DLT is disputed within literature, it is often used interchangeably with blockchain technology (Hileman & Rauchs, 2017; Maull, Godsiff, Mulligan, Brown, & Kewell, 2017; Walport, 2016). Blockchain technology is a subset of DLT that uses a data structure of chained blocks (Ellervee, Matulevicius, & Mayer, 2017; Hileman & Rauchs, 2017). In order to create a clear definition, throughout this paper the term Distributed Ledger Technology (DLT) will be used when referring to the overall technology instead of the more common, but more restrictive, term blockchain technology.

This research uses an approach by Platt (2017) and adapted by Hileman and Rauchs (2017) to define DLT as a number of layers to distinguish the various components of a DLT system. The three 'layers' that are proposed are: protocol, network, and application.

Protocol layer - The backbone on which network and applications are build, the infrastructure.

Network layer - The network that connects participants within a specific protocol.

Application layer - Provides products and services on a specific network, the user interface of a DLT.

Although these layers are not as clear cut as explained above, they do help to understand the different elements of DLTs. In this research the focus will be on evaluating IT risks in the application layer of DLT systems. Inherently this also includes risks in the layers above on which these applications are built.

Blockchain and DLT represent different part of this layered definition. Blockchain can be seen as only one type of DLT. There are new technologies being introduced in the DLT landscape which do not fall under the blockchain definition but do conform to the definition of a DLT. In this research, the following definitions are used, which are further explained in the sections below:

Distributed Ledger Technology (DLT) - *"... all initiatives and projects that are building systems to enable the shared control over the evolution of data without a central party, with individual systems referred to as distributed ledgers"* (Hileman & Rauchs, 2017, p. 24)

Blockchain based protocol - A subset of Distributed Ledger Technology which has *"... global data diffusion and/or uses a data structure of chained blocks"* (Hileman & Rauchs, 2017, p. 24)

Directed Acyclic Graph (DAG) based protocol - A subset of Distributed Ledger Technology which has *"... a directed graph data structure that uses a topological ordering"* (Lee, 2018)

Distributed Ledger Technology is the overarching technology that encompasses technologies like the blockchain. It can be characterized as a shared database without a central validation system and it builds on the assumption that some nodes in a distributed network are malicious (Hileman & Rauchs, 2017; Pinna & Ruttenberg, 2016). Validation of the data often happens by multiple nodes in the network which removes the need of a trusted third party to validate correctness of data. The data of a DLT is distributed across multiple nodes in the network which means there is no single point of failure within the system (Maull et al., 2017). Figure 2.1 visually represents the differences of a centralized ledger with a trusted third party and a distributed ledger. Within the centralized ledger a trusted third party, the clearing house, is needed to perform transactions between parties which do not necessary trust each other. A decentralized ledger removes the need of the clearing house, generating trust between parties which do not trust each other so they can perform transactions directly with each other.

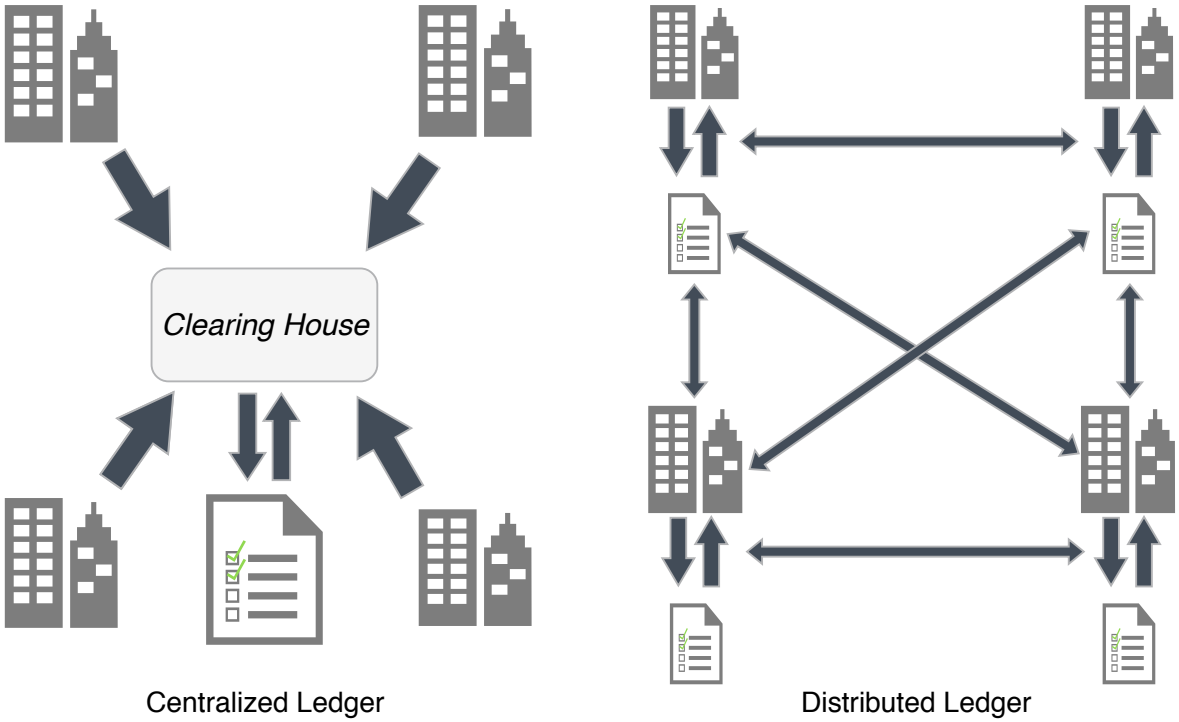

Figure 2.1: Difference of centralized and distributed ledger (Santander Innoventures et al., 2015)

There are a number of different variations of the DLTs which can be useful in different applications depending on the trust of nodes in the network and the anonymity that is needed. In principle, a DLT can be open (public), meaning any participant can read data, or closed (private), meaning only a specific set of participants are able to read data based on certain requirements. Within these categories, there are different sets of permissions for writing and committing to a DLT. In permissioned systems only authorized participants can write and commit, and in permissionless systems any participant can write and commit.

2.1.1 Blockchain

The blockchain is arguably the most well known subsidiary of DLT. It is the technology on which the first public cryptocurrency Bitcoin is built (Iansiti & Lakhani, 2017; Nakamoto, 2008). As mentioned in the definition at the beginning of this chapter, it is built up of blocks that are linked together in a single chain. Multiple transactions are combined into blocks, each with a unique block header. This block header contains the contents of the block, a timestamp and the header of the previous block, thus creating a chain of blocks. Next to this, the block also contains the Merkle root in order to verify the validity of the whole chain without needing to download it all (de Kruijff & Weigand, 2017). This is graphically represented in figure 2.2.

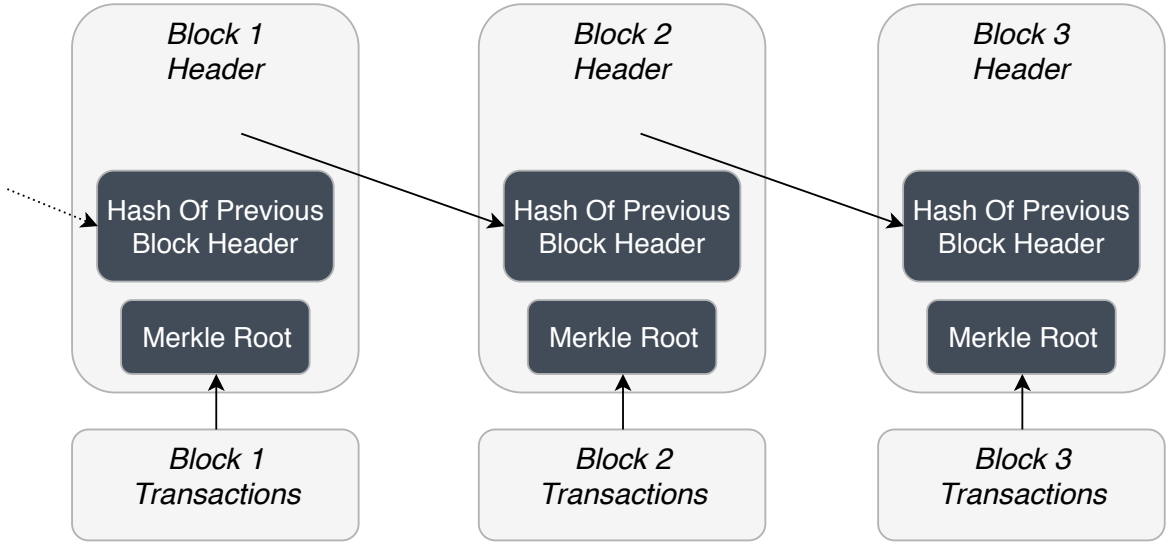

Figure 2.2: Schematic of a blockchain (de Kruijff & Weigand, 2017)

With different nodes all acting on the same data, a method is needed to ensure that the data which is in a distributed ledger has not been altered in any way. A number of ways have been proposed to verify the integrity of a blockchain, Proof of Work (PoW) and Proof of Stake (PoS) proof-of-stake are the most common versions. Proof-of-work relies on computer power to validate integrity of the blockchain. Users in the network, called miners, solve a computationally hard problem, with which they prove that they processed the transaction and that it is legitimate (Babaioff, Dobzinski, Oren, & Zohar, 2012). Proof of Stake does not use computationally hard problems, instead it relies on users putting up a stake, or locking up an amount of their coins, to verify a block of transactions. The cryptographic calculations in PoS are much simpler for computers to solve: you only need to prove you own a certain percentage of all coins available in a given currency. There are different variations based either on proof-of-work or proof-of-stake, relying on different algorithms to achieve consensus.

2.1.2 DAG

Recently, new types of DLT protocols that are based on Directed Acyclic Graphs (DAGs) have been gaining traction. These protocols differ from blockchain based protocols in the way that transactions are linked to each other. Within blockchain based protocols there is one single chain of transactions or blocks while in DAG based protocols there can be a multitude of chains.

A DAG is a directed graph data structure in which the sequence can only go from earlier to later (Lee, 2018). Multiple transactions can take place simultaneously and depending on the protocol, the validation of transactions is done by the transactions themselves and not by separate miners. These differences are essential changes from the blockchain where there is one single 'chain' on which transactions are kept and blocks of transactions can only be created sequentially. Figure 2.3 is a graphical representation of a such a DAG, in which the G is the genesis node; the first node created in a DAG. The genesis node is the only node which does not refer to any other nodes but to which all nodes eventually refer back to.

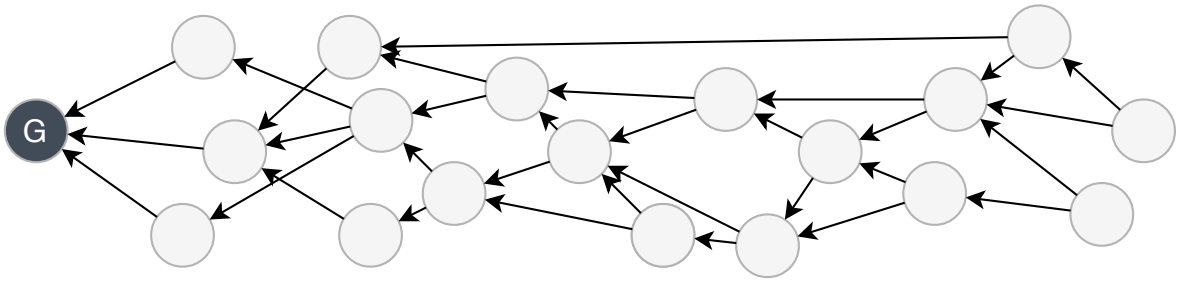

Figure 2.3: Schematic of a DAG (Churyumov, 2016)

Depending on the implementation, validation on a DAG can work differently than within a blockchain. When a node communicates with the network to submit a transaction, it also confirms multiple other transactions at the same time. This can be done using the same protocols as explained in the previous section. This method eliminates the need for separate 'miners' in the network.

There are currently a number of protocols that use this technology; some are fully based on this technology and others use it in combination with other blockchain technologies (Churyumov, 2016; IoT Chain, 2017; LeMahieu, 2014; Lewenberg, Sompolinsky, & Zohar, 2015; Popov, 2017).

2.2 Internet of Things

This section will focus on introducing Internet of Things (IoT) in order to better understand why DLT can play a large role in its future. While exploration in the combination of these two technologies has only just begun, it shows great promise for future applications.

The Internet of Things is a topic that has been gaining interest in the past years. Defined simply, it's a network of interconnected 'things' which were previously not connected. A simple example of a smart home device is a smart lamp, providing consumers with the opportunity to control the lamp from their smartphone or other device instead of a simple light switch. The actual application of IoT devices goes much further than this example, extending to connecting manufacturing plants and even entire cities.

A more extensive and inclusive definition of IoT is given by Gartner as *"the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment"* (Gartner, 2018b). This interconnection of things opens up many new business opportunities for organizations to improve the customer experience for their products or

even to improve their manufacturing processes. In order to do so, organizations need to change their way of offering products to their customers. What was once merely the manufacturing of products, transforms into long time support of these products and offering services on top of these physical products.

In order to support IoT products, an organization needs to support a new technology infrastructure around their products. Figure 2.4 presents all the elements that are needed for successful IoT products according to Porter and Heppelmann (2014). From this technology stack, it is clear that there are many more elements involved than simply the product hardware and software. An organization needs to create a cloud platform with multiple functionalities and create a method of connecting their products to this cloud platform. All of these systems need to work together with their existing business systems and be able to accept information from external sources. Furthermore, customers need to be able to access all the systems through an authentication system. While all these elements do not need to be provided by a single organization, they do need to be in place in order to provide customers with IoT products.

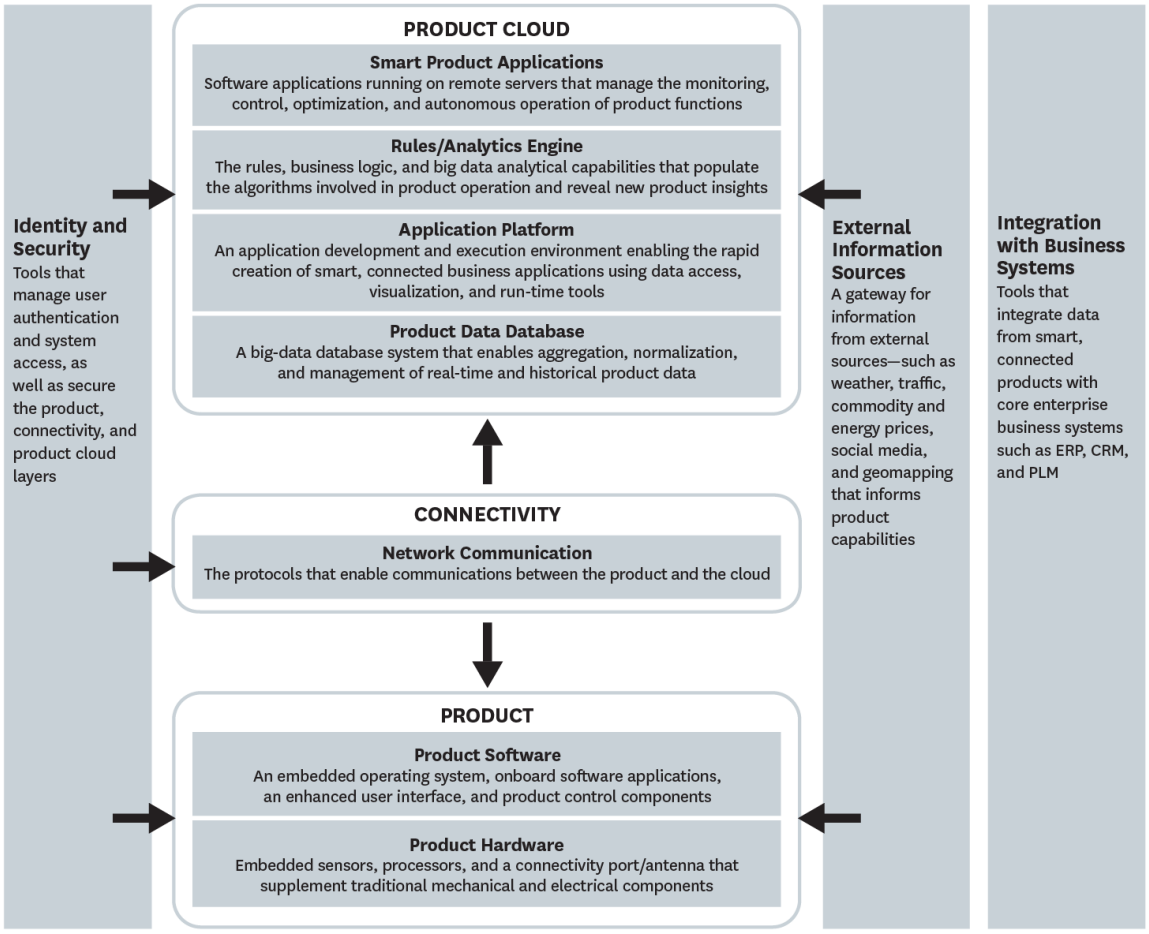

Figure 2.4: Technology stack of IoT (Porter & Heppelmann, 2014)

2.2.1 Challenges of IoT

Current IoT systems have evolved around a centralized model using centralized product clouds to register devices. While this may work for smaller IoT ecosystems, the operating costs and security concerns around this infrastructure increase when the IoT ecosystem grows. The centralized nature of current IoT systems causes them to be expensive due to the high infrastructure and maintenance costs of the centralized cloud solutions (Banafa, 2017). Scaling the systems will cause these cloud solutions to grow even larger and become more expensive. Furthermore, when one of the centralized systems is not available, the entire network can be disrupted as all the communication goes through these centralized systems.

There are currently a number of challenges regarding IoT devices, mostly regarding security of the devices and the information handled by these devices. Securing IoT devices and the surrounding ecosystem create a large challenge for organizations. Currently there are many IoT devices that lack both extensive security measures and life cycle management, creating possibilities for attacks on these devices. Furthermore, in home automation IoT devices, there is a large privacy concern regarding the safety of personal information being saved on the devices or a poorly secured cloud platform. Due to the immature nature of IoT devices, there is currently a lack of security or authentication standards shared by a large number of IoT devices.

A good example of the lack of security in existing IoT devices is a large Distributed Denial of Service attack carried out on October 21st of 2016 targeting Domain Name Systems. This attack was carried out by a botnet largely consisting of poorly secured IoT devices (Symantec, 2016). The botnet used for the attack used weaknesses in the security of IoT devices and default credentials in order to gain access to devices. The attackers were able to shut down or reduce traffic to a number of popular websites for up to a couple of hours. While this attack has awoken customers and organizations about the risks of IoT devices, the situation around poorly secured devices is not resolved yet.

2.2.2 IoT and DLT

Distributed Ledger Technology is presented as a solution for many of the challenges that the IoT ecosystem currently faces. DLT can be seen as a solution to settle privacy and reliability concerns in the Internet of Things (Banafa, 2017). It acts as an enabler for IoT by providing a robust mechanism to support decentralized networks. This decentralized network reduces the single points of failure and the cryptographic algorithms of many DLT networks protect consumer data. Furthermore, it reduces the costs of maintaining a single centralized cloud to support the IoT devices.

The security of IoT devices can be improved by using DLT to perform a number of essential functions. These functions include controlling access, checking and performing software updates, and providing transparency and anonymity for IoT devices. It also opens up the possibility for new business cases using IoT devices. It might for example open up the possibility of using micro-payments between multiple machines or between a machine and a customer without a centralized third party.

While DLT opens up the possibility for many new use cases for IoT, it also comes with a number of limitations that still need to be addressed. IoT ecosystems require a large number of devices to be interconnected with each other but most current DLT systems are not scalable enough to handle this amount of devices. The reduced processing power, battery capacity and networking capabilities of many IoT devices create bottlenecks of running certain types of DLT networks (Fernandez-Carames & Fraga-Lamas, 2018). While research is currently being done to create IoT specific DLT networks (Dorri, Kanhere, & Jurdak, 2017; IoT Chain, 2017), these networks are not mature enough yet to be rolled out in consumer products.

2.3 Maturity Models and IT Risks

When deciding if and how to implement applications within an organization, one aspect that must be carefully considered are the risks associated with the application. With the rapid expansion of Distributed Ledger Technology come many risks as well. These risks associated with the application can be defined as IT risks. There are not many large scale implementations of DLT since many of the applications or networks are not mature enough yet. The development and improvement of applications is rapidly taking place but deciding if an application is ready for large scale roll-outs can prove difficult.

Within literature there are multiple interpretations of the term IT Risks (ISACA, 2009; ISO, 2011; NIST, 2012), but there is no commonly accepted term. Some enterprises put IT risks only as an operational risk while we believe IT risks touch many aspects of different risks. IT has penetrated many aspects of enterprises and therefor the risks related to IT should also be considered throughout these different risk areas. It should not be seen as separate risk, rather as a part of existing risk areas as illustrated by figure 2.5.

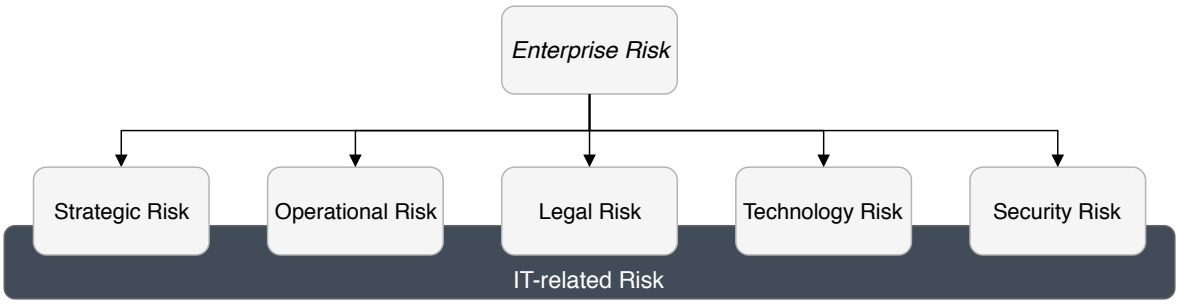

Figure 2.5: IT Risks as part all risks areas

This idea that IT risks are part of multiple risk areas will be used to classify risks associated with DLT applications. In order to aid this classification, the following definition by ISACA (2009) is used:

> *"The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise."*

Assessing these IT risks of a specific application like a DLT application is part of IT risk management. This assessment and managing of risks can be aided with maturity models. Maturity models provide organizations with a method to assess the maturity of a selected domain based on a comprehensive set of criteria (De Bruin et al., 2005).

2.3.1 Defining maturity models

Maturity is defined differently in different fields. In the field of information systems the overall consensus (Lahrmann, Marx, Mettler, Winter, & Wortmann, 2011; Pöppelbuß & Röglinger, 2011) is to use the definition coined by Rosemann and Bruin (2005): "a measure that allows organizations to evaluate their capabilities with regard to a certain problem area." These problem areas can fall in different types of organizational resources which are usually divided into three sections: People maturity, process maturity and object maturity (Mettler et al., 2010). Process maturity is the extend to which a process is defined, managed, measured, controlled and effective. Object maturity is the extend to which a specific object, like a piece of software, reaches a predefined level of sophistication. Finally, people maturity is the extend to which the workforce is able to enable knowledge creation and enhance proficiency.

The idea of maturity models has its roots in models by R. Nolan (1979); R. L. Nolan (1973), where he described a stage model on the progression of IT through organizations. This stage hypothesis has been criticized by multiple scholars (Benbasat, Dexter, Drury, & Goldstein, 1984; King & Kraemer, 1984) but it remains the basis of much research in the IS field due in part to its simplicity. Maturity models became popular in practice with the development of the Capability Maturity Model (CMM) (Paulk, Curtis, Chrissis, & Weber, 1993). This model, developed by the US Department of Defense Software Engineering Institute, has been further developed and adapted into new models over the years (Pöppelbuß & Röglinger, 2011).

The many maturity models that have been created can be used by businesses for multiple purposes depending on the need of the organization. Pöppelbuß and Röglinger (2011) defines three different types of maturity models based on how they are applied in an organization:

- Descriptive - Maturity model applied as an as-is assessment of current capabilities of an entity.
- Prescriptive - Maturity model which indicates how to identify desirable maturity levels and provides specific guidelines on improvement measures.
- Comparative - Maturity model that can be applied for internal or external benchmarking in order to compare maturity levels of similar business units and organizations.

The most basic form and usage of a maturity model is for a descriptive purpose. Comparative maturity models are most complex to create as each organization is different. The criteria for each of these types of maturity models is presented in the next chapter.

Chapter 3

Maturity Models for DLT risk evaluation

To evaluate if current models fit the need for evaluating DLT applications this chapter creates an overview of current relevant models. As presented in the previous chapter, over the years many different maturity models have been developed all with different purposes. Through this landscape of different maturity models it is easy to lose track of what is available and relevant. There are many maturity models of varying quality and varying fields of applicability. This chapter evaluates a selection of models based on quality and relevance to identify the need for a different model.

In order to identify relevant models a literature search for specific maturity models aimed at IT risk maturity of DLT applications has been carried out. The search engines Google Scholar and Scopus are used in addition to the databases of IEEE and ACM. This led to two relevant results based on the title and/or abstract. One of these sources is academic while the other is non academic but upon further research also has an academic basis. This will be explained further in the next section. The models found in the initial search are the following:

- Maturity Model for Blockchain Adoption (Wang, Chen, & Xu, 2016)
- KPMG Blockchain Maturity Model (KPMG, 2017)

In order to gather more models which might be relevant to the research we broadened the search to also include general and/or IT specific risk management maturity models not directly related to DLT. A selection of well known maturity models with risk management aspects have been included in this analysis:

- CMMI for Development v1.3 (CMMI Product Team, 2010)
- Risk Maturity Model (RIMS, 2006)
- IT Capability Maturity Framework Risk Management (Carcary, 2013)

These models have been chosen because these models all have a different degree of generalizability in business contexts. CMMI for Development (CMMI-Dev) has a high level of generalizability as it can be applied to many different processes within an organization. On the other side of the spectrum is the KPMG model which is very specific as it can only be applied to analyzing IT risks of blockchain applications. In the following sections each model will be explained in more detail. The order of models will be from general maturity models to more specific maturity models.

3.1 Overview of Maturity Models

3.1.1 CMMI for Development 1.3

The CMMI-DEV model is aimed to guide process improvement across a project, division or an entire organization (CMMI Product Team, 2010). The model aims at covering multiple processes within an entire organization. Some of the areas on which the CMMI focuses can therefor be very abstract in order to cover a large number of practices.

The CMMI model is most well known in the industry, it is used as a basis for multiple other models as well (Becker et al., 2009). It is developed at the Software Engineering Institute of the Carnegie Mellon University and its development traces back to 1987. Through the years multiple models have been released improving on the previous versions.

The CMMI-DEV model is divided into 22 process areas, each area contains a cluster of related practices that when implemented collectively, satisfies a set of goals considered important for making improvement in that area (CMMI Product Team, 2010). For the purpose of this research we will focus on one of the process areas namely Risk Management (RKSM).

It should be noted that at the time of writing the CMMI-DEV 2.0 has been released. This model is the first update after 8 years but for the first time it is not available for free. Even though changes to this model are significant, for the purpose of this research it is expected to not be of influence. Because of this reason, along with the costs associated with using the new model, the 1.3 version of the model will be used for this research.

3.1.2 Risk Maturity Model

The Risk Maturity Model (RMM) is a model which combines elements from different models and standards into one model. It is aimed at Enterprise Risk Management (ERM) practitioners and aims to offer a method to evaluate and set goals in terms of risk performance (RIMS, 2006). It is focused only on risk management and mainly on an enterprise level.

The model is created in 2006 by LogicManager in collaboration with the Risk and Insurance Management Society (Risk Management Society, 2018). It is based on the methodology of the CMM model and has therefor the same levels as the CMM model.

The RMM consists of seven attributes which fit in existing frameworks like COSO ERM, and COBIT. Attributes consist of subjects like ‘ERM process management’, ‘Uncovering risks’ and ‘Root cause discipline’, among others. In order to further specify risk management within these attributes there are 25 competency drivers consisting of a total of 68 key readiness indicators to measure these competencies.

3.1.3 IT Capability Maturity Framework Risk Management

Managing IT specific risks is well discussed in literature but there exist relatively few maturity models aimed specifically at IT risk management. Most literature is in the form identifying IT risks or best practice frameworks like the IT risk management framework Risk IT by ISACA (2009). These frameworks do however not provided the added benefits of a maturity model like providing a path for improvement.

Carcary (2013) has provided an IT risk management maturity framework which is part of the IT Capability Maturity Framework (IT CMF) by Curley (2008). The IT CMF consists of 33 critical capabilities of which risk management is one, Carcary (2013) focuses on this capability. The risk

management capability consists of ten capability building blocks which consist in turn of multiple dedicated maturity questions.

3.1.4 Maturity Model for Blockchain Adoption

Wang et al. (2016) have created a maturity model for blockchain adoption. While this is a blockchain specific maturity model, it is not very extensive. It identifies the current maturity of blockchain protocols in general. It states that the maturity of the blockchain is currently not high enough yet and provides some recommendations to organizations choosing to adopt blockchain applications.

3.1.5 KPMG Blockchain Maturity Model (BMM)

KPMG has created a maturity model for analyzing risks of blockchain application adoption. This model can be used to assess the state of a DLT implementation and how well certain DLT-specific IT risks are under control (Spenkelink, 2017). The exact content of the model is not available to the public, however, through contact with KPMG more details about the model have been collected. An adaption of the paper on which the model is based is published in (van der Voort & Spenkelink, 2018). Using this model and an interview held with one of the authors of the model this maturity model is further evaluated.

While there has been research about risks of blockchain and implementing blockchain technology in businesses, this has been relatively scattered or only applies to a small niche in the market. The model by KPMG has created a comprehensive overview of the IT risks involved in implementing private DLTs and is created for and verified within the financial services industry (Spenkelink, 2017). A literature review has been carried out to identify current IT risks and these have been categorized into eight risk areas. Each of these risk areas is divided into multiple sub risks which are in turn measured using maturity self assessment questions. Each self assessment question relates to an IT risk area and is assigned to a specific maturity level. These questions and corresponding levels have been created in collaboration with experts within KPMG and the financial services industry.

3.2 Evaluation of Maturity Models

To evaluate the maturity models that are mentioned in the previous section we will look at two different aspects of the models, the applicability and the quality of the models. Quality of models is a heavily debated issue within IS research (De Bruin et al., 2005; Mettler et al., 2010; Pöppelbuß, Niehaves, Simons, & Becker, 2011), many authors argue that research rigor is often times not carried out successfully. A method to create maturity models by rigorously executed design science research has been proposed by (Becker et al., 2009). In order to evaluate the quality of maturity models Pöppelbuß and Röglinger (2011) has proposed a number of design principles that can be used to develop and evaluate maturity models.

The applicability of maturity models on specific applications is less discussed in literature. While there is a consensus that there are many different models available and some are very similar, a comprehensive method to choose a specific model has not been proposed yet. Mettler (2011) has made suggestions as to criteria for maturity model selection. These can be used to evaluate the applicability of the selected maturity models to the identified problem area.

The criteria that will be used to evaluate the methods have been extracted from the papers of Mettler (2011) and Pöppelbuß and Röglinger (2011). They are combined to the following criteria:

- Applicability
  - Origin of the model
  - Reliability
  - Accessibility
  - Practicality of recommendations
  - Method of application
  - Design mutability
- Design principles
  - Basic
    - Basic information
    - Definition of central constructs related to maturity and maturation
    - Definition of central constructs related to the application domain
    - Target group-oriented documentation
  - Descriptive
    - Intersubjectively verifiable criteria for each maturity level and level of granularity
    - Target-group oriented assessment methodology
  - Prescriptive
    - Improvement measures for each maturity level and level of granularity
    - Decision calculus for selecting improvement measures
    - Target group-oriented decision methodology

For each model presented in the previous section these criteria will be used for evaluation. The complete notes of the evaluation can be found in appendix A. In table 3.1 an overview of the results of the evaluation are presented. CMMI-Dev v1.3 is qualitatively a very good model that is in use within many different companies and is freely accessible. Appraisals take place by professionals according to Appraisal Requirements for CMMI which includes general recommendations of process improvement. All basic and descriptive design principles are included in the model, not all prescriptive principles are included but these principles might be included in appraisals of the CMMI model.

The Risk Maturity Model (RMM) is based in practice created by Logicmanager. It has been verified at a large number of organisations and validated in a single research paper. The model itself is not available for free, a small self assessment is available for free. The recommendations are general on processes of risk management. From the information that was freely available it can be deduced that all basic and descriptive principles are included in the model. Only the inter subjectively verifiable criteria are unknown based on the information available. The prescriptive principles are not all included, missing a decision calculus and a target group decision methodology.

The IT CMF model is based in academics and further developed in practice. The model is verified in practice but not validated and it is not available for free. Only academic papers can be found with parts on the model. The recommendations by the model are problem specific and assessments are carried out by third parties. All the design principles are included in the IT CMF model.

The Blockchain Maturity Model is very limited in its applicability and information. It is an academic model but it is not verified or validated. It offers a very general overview of the maturity of blockchain in general. Almost none of the design principles are included, only the basic information and target group documentation is available.

The KPMG Blockchain Maturity model is based in academic research into the IT risks of blockchain of which the full research is not available to the public. It is verified through case studies but the step from individual risks to maturity levels is not clear from the available literature. Assessment is done in collaboration with KPMG after filling in an assessment. The recommendations from this assessment are very specific to the problems identified. The model includes many of the basic and descriptive design principles, although not all elements are clear from the available research. The prescriptive design principles are not included in this model but it might be possible that these elements are included in the consulting services of KPMG.

3.3 Conclusion

The current landscape of maturity models is very broad with models operating on different levels of analysis. In this research a solution is being sought for evaluating specific DLT applications using a maturity model. While some of the identified maturity models that have been evaluated are of good enough quality, only the KPMG Blockchain Maturity model fits the purpose of evaluating a single DLT application. Other models are either too broad or do not offer enough guidance in evaluating the risks related to DLT applications.

The KPMG model is not available to the public and the complete academic background cannot be verified. It is also focused on the financial technology sector which may have some different requirements than the IoT sector. While the model is able to evaluate specific DLT applications, we believe additional benefit can be had from a publicly available model fit for IoT applications.

Table 3.1: Comparison of different maturity models

Criteria	CMMI-DEV v1.3	RMM	IT CMF	BCMM	KPMG BMM
Applicability					
Origin	Academic	Practitioner	Academic	Academic	Academic
Reliability	Validated	Validated	Verified	None	Verified
Accessibility	Free/Charged[a]	Charged	Charged	Free	Charged
Practicality	General	General	Specific	General	Specific
Method of application	Certified professionals	Self-assessment	Third-party assisted	None	Third-party assisted
Design mutability	Form and functioning	Form	Form and functioning	Form	Form and functioning
Design Principles					
Basic principles					
Basic info	++	+	+	+	+
Definition of constructs related to maturity	+	+	++	-	+/-[b]
Definition of application domain	++	++	++	- -	++
Target group documentation	++	++	+	+/-	+
Descriptive principles					
Intersubjectively verifiable criteria	++	?[c]	+	-	++
Target group assessment methodology	++	+	+	- -	+/-
Prescriptive principles					
Improvement measures	+	+	?[d]	- -	+/-
Decision calculus	-	- -	+	- -	-
Target group decision methodology	-	- -	+	- -	- -

[a] The v1.3 model is available for free but the newest v2.0 model is charged.
[b] Full documentation not publicly available
[c] Documentation not freely available
[d] Documentation not freely available

Part II

Design

Chapter 4

IT Risks Described in Literature

With the need of a new model established, we start to identify what is needed to design the model. In this chapter the IT risks related to Distributed Ledger Technology are identified through a literature study which is complimentary to a study already executed by van der Voort and Spenkelink (2018). This study is brought up to date and an additional search for risks specific to IoT has been executed. This resulted in a collection of 29 individual risks divided over five areas.

4.1 Literature Study

This literature study followed a semi-structured approach. It attempts to cover all relevant papers in order to collect IT risks of DLTs. The literature review is carried out according to the Preferred Reporting Items for Systematic Reviews and Meta-Analysess (PRISMAs) approach (Moher, Liberati, Tetzlaff, & Altman, 2009). This is a method to carry out a thorough systematic literature review. In this research not all steps of the PRISMA approach are completed, the qualitative synthesis and meta-analysis are excluded. Instead of these last steps we are analyzing the primary papers and extracting only IT risks from these papers. A systematic literature review approach is chosen in order to include as many as possible papers about IT risks of Distributed Ledger Technology.

A literature review close to the topic of this review has already been carried out by van der Voort and Spenkelink (2018), this review covered risks of DLT but did not cover IT risks of DLT in the IoT field. The full results of the literature review form van der Voort and Spenkelink (2018) are also not available. The keywords from this study are adapted in order to also cover IoT risks. Furthermore, a search has been carried out in Elsevier Scopus in order to obtain more papers. The main keywords are related to the three main themes of this research: Distributed Ledgers, Internet of Things and Risks. From these main keywords a number of similar keywords were identified which are used to formulate a search string. The keywords used for the search are listed in table 4.1.

IT risks of DLT applications in general are inherently also risks which are applicable to DLT applications in the IoT domain. Therefore in this literature review two search terms will be used to collect relevant articles. While the only difference of the search query is the addition of IoT keywords, this produced different results than searching for IoT keywords within the results of the general query. This is likely due to the way the search engines for specific databases are set up.

The search engines Scopus and Google Scholar and the databases of IEEE and ACM are used to find relevant articles. The Science Direct database is excluded from this search since these articles are also included in the Scopus search engine. The results from the initial search query are narrowed down first by title and the remaining papers by relevance of the abstract. Because of the large amount of results in the Google Scholar search engine, only the first 10 pages (100 results) of the results

Table 4.1: Keywords utilized in the literature study

Distributed Ledger	Internet of Things	Risks
DLT	IoT	IT risks
Distributed Ledger Technology	Embedded Systems	Disadvantage
Blockchain		Risk management
Block chain		Threat
		Weakness
		Vulnerabilities
		Challenge

will be included. Additional papers from forward/backwards citing and recommendation engines from Mendeley are also included.

In figure 4.1 the result from each stage in the literature study is visualized. Each number in the diagram represents the number of papers included in the step. In the selection of titles a relatively broad selection of papers has been made. This is because in an initial search it has been found that there are many articles that cover some detail on risks or challenges of DLTs but do not have it as their main focus. Therefor the title may not reflect some of the relevant information in this research. The titles that were included relate to challenges and risks with different types of DLT or to the connection between IoT and DLT.

The selection on abstracts looked at the abstract or introduction and headers of different sections of the paper or article. Papers were included in the selection when they showed they had connection with risks of DLTs or challenges related to them.

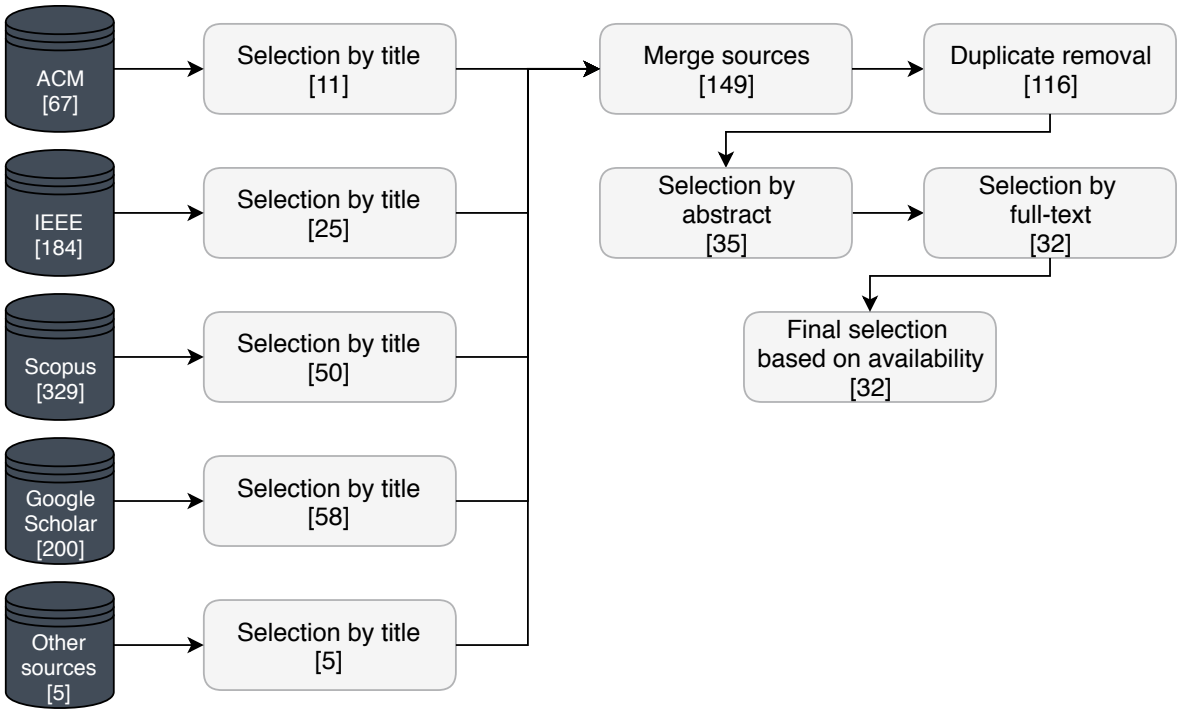

Figure 4.1: Diagram of papers collected through systematic review

In appendix B.1 the primary list of papers which are included in the literature review is presented. From the results of the literature study it becomes clear that the research in this area has only recently gathered the interest of researchers. Figure 4.2 presents the years in which the selected papers have been published. It is interesting to see that no papers older than 2016 have been included and that the amount of papers almost tripled in the year 2017. Even though the literature search has been performed in may 2018, the amount of relevant papers is already as high as in 2016. One reason for the recent increase in interest might be because of a shift in focus on the topic. In the past, research has been focused on creating use cases and evaluating and improving the technology itself. Recently, there has been a shift towards implementing these systems within companies which in turn increases the need to look into the related IT risks.

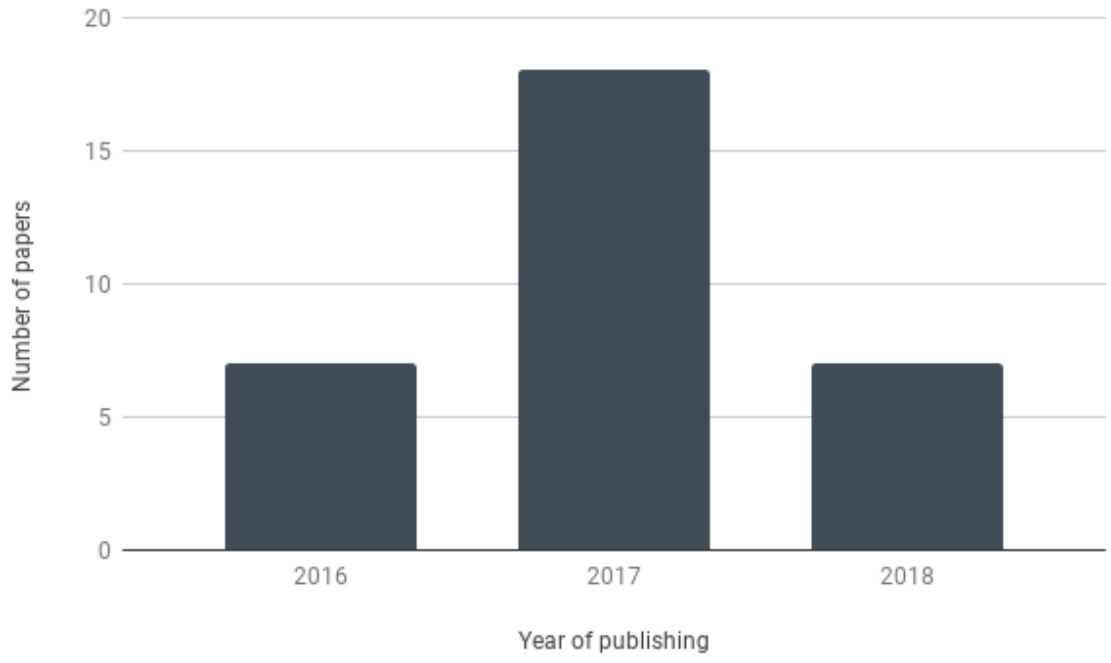

Figure 4.2: Year of publishing

4.2 Extracting and classifying risks

The goal of the literature study is to identify the different IT risks related to DLT for IoT within literature. At first a list of all the risks mentioned in the papers are extracted, from each risk it is noted from which papers they have been deduced. This total list of risks consists of 57 individual risks of which some are related but not duplicate.

In order to create a better overview of the risks some additional processing has been done. The risks have been analyzed in a mindmap to deduce multiple categories within the risks. Risks that relate to each other were grouped together and a common theme between these risks was found. A total of 5 categories have been defined through this analysis. These categories are the following:

- Strategic Risks
- Operational Risks
- Security Risks
- Legal Risks
- Technology risks

The different risks within the risk categories have been consolidated to further group together similar risks. This resulted in a final collection of 29 different risks. Figure 4.3 presents the different steps of the identification process and the number of risks that were carried on from each step. The list of consolidated risks derived from literature including from which papers they stem can be found in appendix B.2.

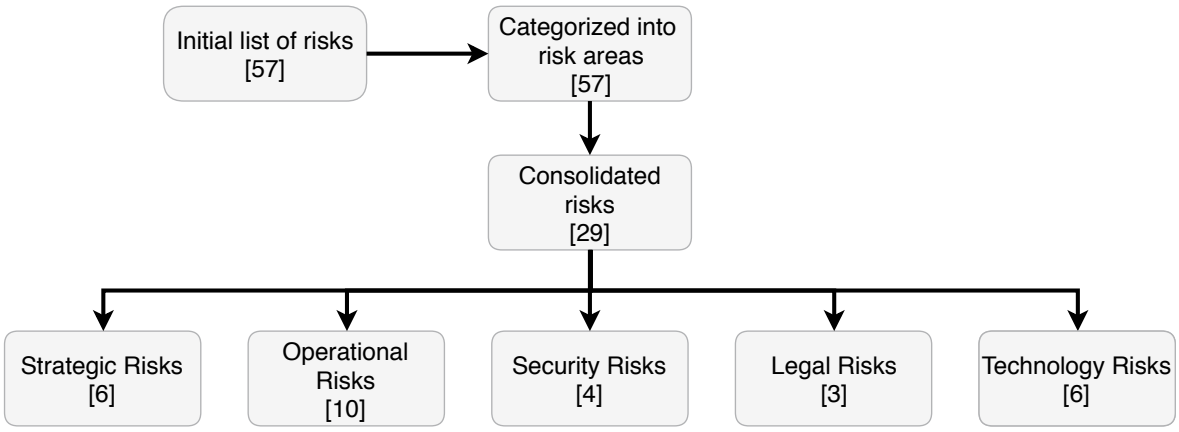

Figure 4.3: Overview of the different steps of collecting the risks

Chapter 5

IT Risks Described by Field Experts

In order the create a more complete collection of risks, a number of field experts have been consulted to verify and adapt the identified risks from the literature study. A two round Delhpi study has been performed which resulted in a preliminary risk model for further evaluation during a number of case studies.

5.1 Study Design

In order to identify IT risks of DLT applications according to field experts, a Delhpi study has been set up. According to Okoli and Pawlowski (2004) the Delphi method leans itself for concept/framework development study following a two-step process namely: identification and elaboration of a set of concepts, and classification and taxonomy development. This approach fits well with the creation of a maturity model as exemplified by a number of maturity model creation studies (De Bruin et al., 2005; Mettler, 2011; Rosemann & Bruin, 2005; Smits & Van Hillegersberg, 2015; Van Dijk, Willem, Van Hillegersberg, & Daneva, 2017). According to Hasson, Keeney, and Mckenna (2000), the Delphi technique is particularly useful in areas of limited research; as is the case for DLT related research. Furthermore it is suited to explore areas where controversy, debate or a lack of clarity exist. This fits perfectly with the current landscape of DLT research, as there are many different opinions on the design and risks relating to DLT applications.

There are a number of different ways to conduct a Delphi study but the techniques all aim for the same goal as characterized by Linstone and Turoff (1975):*"Delphi may be characterized as a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem."* The traditional Delphi method was developed by Norman Dalkey of the RAND corporation in the 1950's (Dalkey & Helmer, 1963). Rowe and Wright (1999) note that a classical Delphi study should consist of four key features: anonymity of Delphi participants, iteration, controlled feedback, and statistical aggregation of group response. The traditional way of conducting a Delphi study is by collecting a number of experts in the same room for a day and having them reach consensus during a number of rounds. However, in order to meet the requirements of a given study, Linstone and Turoff (1975) argue that a Delphi method can also be adapted. For this research the approach of Skulmoski, Francis Hartman, and Krahn (2007) will be used to conduct the study, using questionnaires for a geographically dispersed group of experts.

A two round design has been chosen based on the design used by Rosemann and Bruin (2005). We have excluded ranking the different risks and creating level descriptions which are the third and fourth round of the Delphi study by (Rosemann & Bruin, 2005). This approach has been chosen because of the difficulty of generalizing level descriptions for a number of the identified risk areas

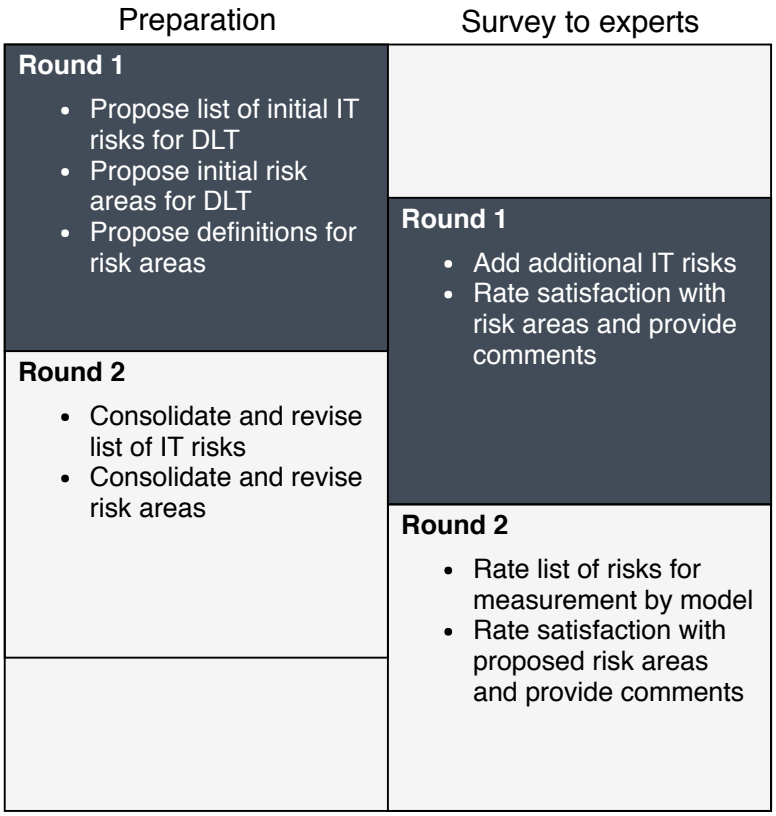

Figure 5.1: Study design of the Delphi study

during the first rounds of the Delphi study.

During the two rounds, IT risks that are identified in the literature study are adapted and further classified. Figure 5.1 illustrates the design of the two rounds of the study where in the left column the work by the researcher is explained and the left the task for the experts. The first round of the study focuses on brainstorming around the risks and risk areas that have been identified in the literature study. The second round verifies the adapted lists and rates the satisfaction with the newly proposed risks and risk areas.

5.2 Selection of Experts

One critical component of the success of a Delphi study is the selection of experts, after all, it is the opinion of these experts that shapes the result of the study. Experts must have expertise in the subject of the study and be able to provide relevant insights to the topic. While in most surveys the opinion is sought of a representative sample of a population, this is not the aim of a Delphi study. All the participants of the panel should adhere to a number of criteria in order to be considered experts. There is a debate in literature about how to select experts in a Delphi study and what criteria should be used to select the experts Devaney and Henchion (2018). In this research the criteria for ‘expertise’ as presented by Skulmoski et al. (2007) is used. These criteria are the following:

Sector of focus	#
IT Consulting	3
Automotive	2
Logistics	4
Energy	2
Manufacturing	4
Cyber security	1
Academics	2

Table 5.1: Sector of participants

Function	#
Academic researcher	2
Software Architect	2
R&D and Strategy Manager	3
IT Consultant	3
Business partner manager	1
Researcher in DLT-related research unit	4

Table 5.2: Function of participants

1. Knowledge and experience with the issues under investigation
2. Capacity and willingness to participate
3. Sufficient time to participate
4. Effective communication skills

Based on these criteria a list of potential experts have been identified. The potential experts have mostly been collected through contacts in the Netherlands and Germany and snowballing further to reach other candidates. A list of 30 potential candidates have been contacted and 15 candidates have agreed to participate in the study. The other potential candidates either did not respond or stated that they did not have the time to participate. The experts that have agreed to participate in the study are distributed across multiple countries, multiple companies, multiple disciplines and have different relations with the topic. This distribution is important since it increases the possibility of different opinions on the topic. In table 5.1 and 5.2 the number of experts is shown according to their expertise, the IT consultants have been divided further based on their sector of expertise.

5.3 Conducting the study

The Delphi study technique using surveys can be conducted in a multitude of ways. Traditionally the experimental studies have relied on paper based surveys sent out to participants, later this transformed into to electronic based surveys through email or online surveying tools (Hasson et al., 2000). However, with these methods it is difficult for participants to respond to each other during a survey round, which is one of the advantages of performing a Delphi study in-person.

In order to reproduce the behavior of a local condensed group of experts in a geographically dispersed group of experts through an electronic way, a Group Decision Support System, Spilter, is used (Spilter, n.d.). This online tool provides the possibility of viewing anonymous answers from other participants in the study while the survey is being conducted.

5.4 Delphi Round 1

The first round of the Delphi study was filled in by fourteen out of the fifteen participants on time. One participant was not able to participate because of a lack of time. He noted that he would like to be included in the following round. A summary of the results of this round has been sent to him to provide him the insights gathered during round 1.

The focus of this round is to identify additional risks to the ones that have already been identified in the literature study. The survey of round one was divided into three parts and had a combined total of 11 questions. The first part focused on gaining some more demographic information about the participants. Part two included five questions, one for every risk area as defined in the literature study. Participants got the opportunity to add their own risks and note if they don't agree with any of the proposed risks in each risk area. Part three of the survey offers the opportunity to comment on the identified risk areas. For each risk area the participant was able to note on a five point Likert scale if they agree with the definition or not. When they do not agree with a definition of a risk area they had the opportunity to propose one themselves. The last question of the survey asks the participant to note on a five point Likert scale if they agree that the list of risk areas is complete or not. The full survey can be found in appendix C, section C.1.

5.4.1 Redefining Risk areas

The participants were asked if they agreed with the defined risk areas and if the proposed risk areas were complete. While half of the participants agreed that the list was complete (7 out of 14), the remaining participants either disagreed or neither disagreed or agreed with the completeness. The comments given with the scores provide some insights as to why participants scored the question low:

> *"Some risks may overlap, for example: 'a low number of nodes in a network' can be classified as a Technology and Security risks."*

> *"In general they are OK, but I question if this provides any insights based on a lot of the answers as filled in before."*

Based on these comments and other suggestions, the risk areas have been redefined to create less overlap and to be able to provide more insights. In order to achieve this, a new layer has been added to the model. This new layer provides more insights in the topics covered by the different high level risk areas and provide a method to further categorize risks. Furthermore this layer aims to create a more clear divide between the high-level risk areas.

The high-level risk areas have been redefined based on the feedback from the participants. The lowest scoring and most controversial risk area, technology risks, has been replaced by two new risk areas: 'Development' and 'DLT platform selection'. These areas in part cover some of the risks previously categorized in the 'Technology' risk area. In figure 5.2 the redefined risk area model is presented with it's 6 high-level risk areas and 23 newly defined low-level risk areas. These risk areas are proposed to the participants in the second round of the study.

5.4.2 Redefining IT Risks

During the second part of the first round the participants were presented the list of 26 risks as identified in the literature study. They were asked if they agreed with the list of risks and if they had any additional risks which were not mentioned. While the participants did not disagree with the risks already identified, they provided an additional 110 risks bringing the total up to 136. This large increase may partly be explained by the varying abstraction level of the identified risks.

In order to decide an abstraction level for the use in this model, guidelines from De Haes et al. (2009, p. 56) are used. Based on these guidelines it has been decided to use a relatively high level of abstraction for the risks in order to retain a manageable number of risks and to be able to provide

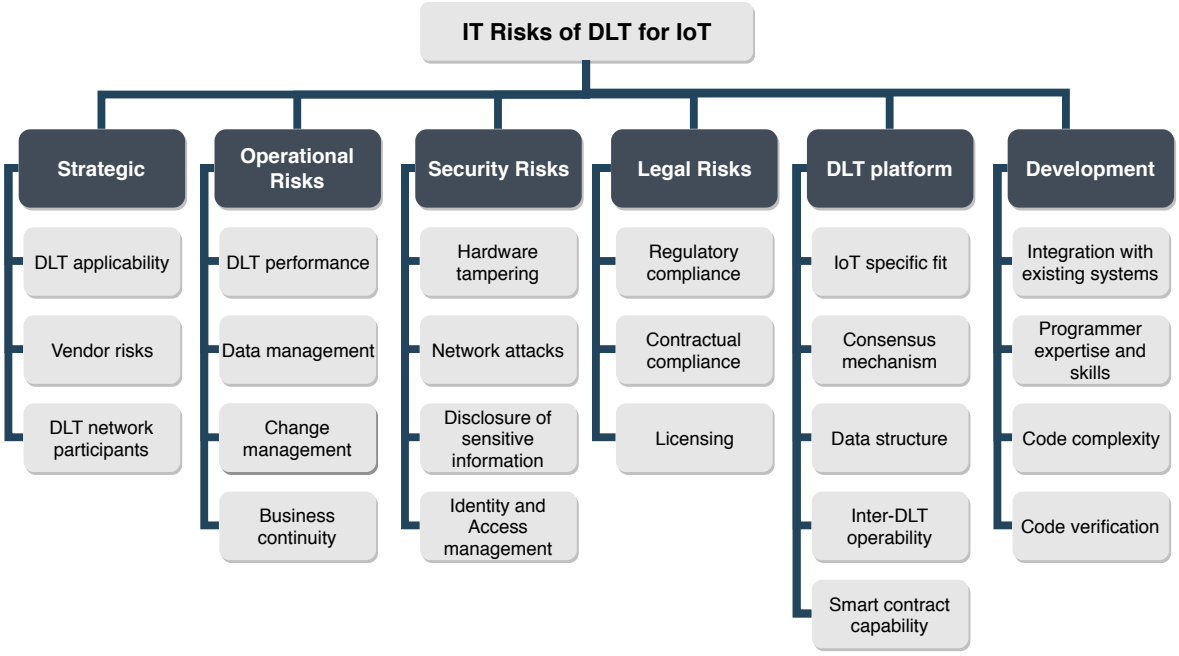

Figure 5.2: Redefined two layer model after round 1

the best insights from the model. In order to explain the generalizations a description is added to each risk. This brought down the list of risks form 136 to 66 risks divided over the newly defined 23 low-level risk areas. These risks are again presented for validation in the second round of the Delhpi study.

5.5 Delphi Round 2

The second round of the Delphi study was filled in by thirteen out of the fifteen participants on time. One participant, a different one than in the first round, stated that he did not have enough time. The other absentee was on vacation during this time, he communicated this before agreeing to participate in the study. A summary of the results of this round has been sent to both participants to provide them the insights gathered during this round.

The second round of the Delphi study focused on validating the redefined risk areas and risks stemming from the first round of the Delphi study. The first part of the survey provided participants the opportunity to give feedback to the newly defined risk areas and sub-risk areas. For each risk area and corresponding sub risk areas the participants were able to state their satisfaction with the redefined areas. In the second part of the survey the participants were asked for each risk if they wanted to include or exclude the proposed risk in the model. The complete survey can be found in appendix C, section C.2.

5.5.1 Evaluating Risk Areas

The risk areas which have been adapted based on the outcomes of the first round were presented to the experts for validation. For each risk area they were given the opportunity to rate their satisfaction with the risk area on a scale from 1-5 with 1 representing 'Strongly disagree' and 5 'Strongly agree.'

Each of the redefined risk areas have been rated with an average of 4.0 or above, it can be deduced that on average the participants agreed with the defined risk areas. Table 5.3 shows the

results of the ratings given by the panel members. However, there were a number of risk areas with a higher spread of ratings than others. One risk area which had this high spread is the legal risk area, with a spread of 0,96 the highest of all the risk areas. This is mainly due to two ratings of participants that disagreed with this risk area and rating it with a 2. From the commentary it becomes clear this is due to the fact that privacy regulation is not clearly stated in this risk area. They would see more benefit in a model which breaks down the compliance with specific regulation, for example General Data Protection Regulation (GDPR), instead of having one general area of regulatory compliance:

> *"Breakdown Regulatory (Data location, Data storage, GDPR (right to get forgotten)..."*

> *"Adding privacy compliance would be good."*

The breakdown of regulatory compliance or privacy compliance is not included in the model in detail on purpose. Specific rules for compliance are not clear yet and are rapidly changing. Therefor the choice has been made to mention the different regulations in the description of the risks and not breaking down compliance with these specific regulations further. A more in depth look into regulatory compliance should be done during the evaluation of an application. This should be looking into not only GDPR and Data location regulation but also including different regulations regarding monetary regulation like Anti Money Laundering (AML) and Know Your Customer (KYC) regulation.

Other risk areas which have been taken a closer look at are the security and DLT platform risk areas. Within the security risk area the commentary mostly relates to the lack of a specific privacy related risk area and some disagreement on using the division of hardware/software tampering. The abstraction level of the sub-risk areas are also a point of discussion with some of the areas being very generic while others are quite specific. The sub-risk areas in the security area have been redefined to reflect the commentary given.

> *Translated: "Hardware and Software tampering are quite generic; I would change the word tampering to something like risks. Other than that it's pretty high level with one or two specific sub areas. Either remove these or make the rest also more specific."*

The DLT platform area showed some uncertainty if this is actually a category by itself or if it can be placed under other risk areas. The commentary is also given that this risk area overlaps quite a bit with the other risk areas. Based on this commentary the decision has been made to remove this risk area and place its contents under the strategy risk area.

> *"I'm not exactly sure if DLT platform is a risk itself or that the sub-risks should be placed under the other risk areas. The risks areas seem to be quite overlapping."*

Based on the commentary given on the risk areas during this round, the risk areas have been redefined. The redefined risk areas are presented in section 5.6.

Risk area	Average	Spread
Strategic	4,08	0,47
Operational	4,31	0,46
Security	4,08	0,83
Legal	4,00	0,96
Development	4,15	0,53
DLT platform	4,08	0,62

Table 5.3: Results of risk area satisfaction rating

5.5.2 Evaluating Risks

In the second part of this round the list of risks expanded from the previous round was presented for validation by the experts. These risks were rated by the panel on a three point scale (1-must stay, 2-either way, 3-can go) based on the scale used by (Rosemann & Bruin, 2005).

The risks that were presented to the participants were divided into each of the different risk areas. While most risks averaged above a 2.0, a number of risks scored below a 2.0 or are really close to averaging 2.0. When a risk on average scored below a 2.0 they are removed from the model. The risks that were close to dropping below this threshold, scoring below a 2.2, were further examined to see if they should still be included in the model.

During further examination of the low scoring risks and consultation with a field expert which was not included in the Delphi study, a possible explanation of the low scores has been identified. The descriptions of most of the risks are quite summarily and sometimes do not cover the precise intended meaning. The complete list of risks has been further examined during this process and more detailed explanations of the risks are created. A total of 48 detailed risks remained which are included in the preliminary model to be tested during a number of use case studies.

5.6 Preliminary model

Based on the outcomes of the Delphi study a preliminary risk model has been created. This model includes all the additions proposed during the Delphi study and has only included risks which have been agreed with by the participants. Figure 5.3 shows the current overview of the different risk areas and sub risk areas. The risks will be further evaluated for fit in practice by applying them to a number of case studies.

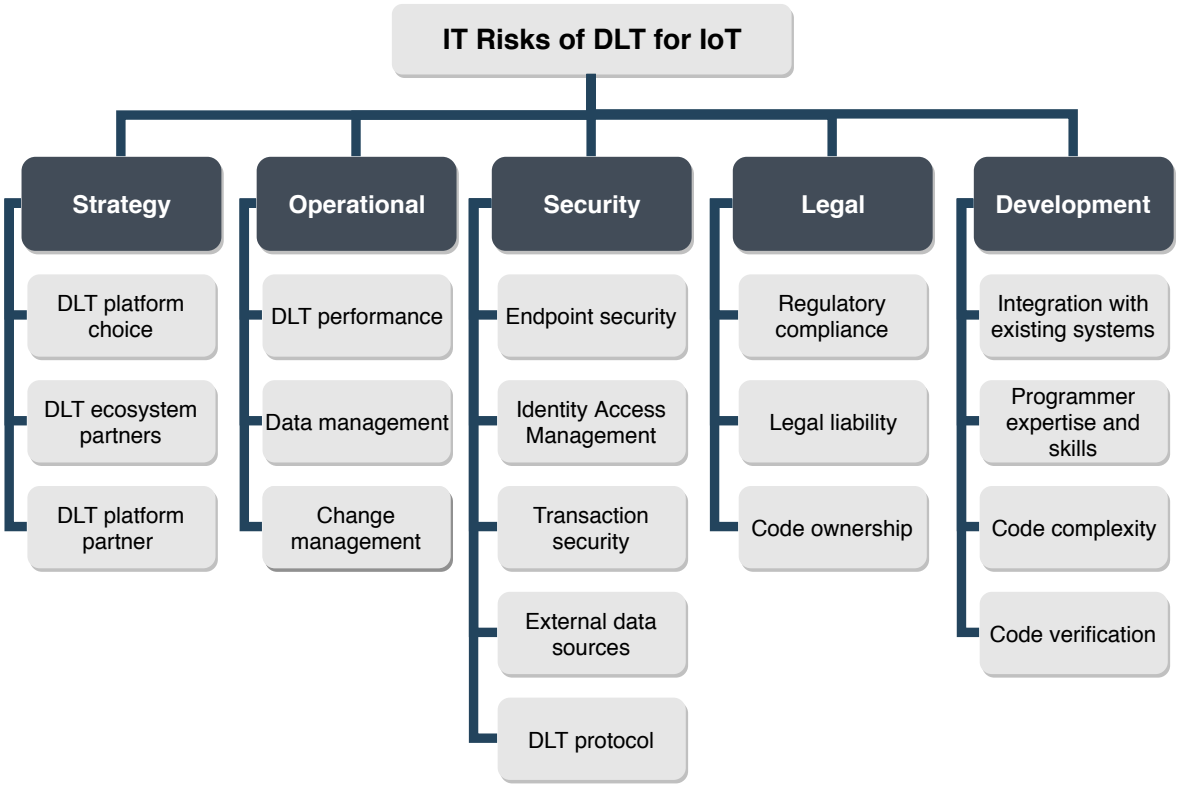

Figure 5.3: Preliminary Risk Area model

Chapter 6

Case Studies verifying Risks

In order to further evaluate the risks and see how they apply to practice, a number of case studies have been performed. A total of four projects have been evaluated, these projects are in different stages of development and include a multitude of stakeholders from different companies. This chapter lays the groundwork for the next chapter where a maturity model is formed based on all the findings during the previous stages of the study.

6.1 Introduction

In order to verify the list of risks as identified in the literature study and the Delphi study, a number of case studies are performed. The case studies will be observed without performing an intervention, interviews will be performed guided by the findings of the research so far. This approach to the case study most closely correlates to the classification of an observational case study as presented by Wieringa (2014). The case studies have been set up according to the principles presented in this book. The aim of the case studies is to answer two questions about the preliminary model. First, the question of how the identified risks correspond to risks already identified in the projects. Second, how the model can be adapted to better suit the needs during development of the application.

6.2 Case Study Design

As mentioned in the introduction the design of the case studies will follow the principles of a single-case mechanism experiment as defined by Wieringa (2014). What will be investigated during the case studies are application development projects which use DLT to perform a function within the application and have at least a proof of concept to evaluate. During the case studies we will evaluate how the preliminary model can be used to add benefit during and after the development of a DLT application.

The preliminary model with underlying identified risks will be used as a guideline to assess the applications and the business processes surrounding the applications. Each identified risk has been given a more complete description in order to better guide the evaluation. A number of different structured interviews with stakeholders in the project are administered. The stakeholders that will be interviewed are developers of the application, product owners and managers deciding the course of the development process. After the interviews, an assessment was created in order to identify how the different risks of the preliminary model are handled within the application.

6.2.1 Selection of Cases

In order to find relevant cases to evaluate, the population from the Delphi study has been asked for their involvement in projects where an application is being developed which uses DLT. Furthermore a number of other contacts have been contacted in order to gain a larger number of case studies. From these requests a total of five cases have been provided which fit well with the case study.

The identified case studies have different stages of development, with one case study close to being in production and another one creating a Minimal Viable Product (MVP). This allows us to further evaluate how the model functions within these different stages of development and where it can be most useful.

6.3 Supply Chain Management

In this case study a closer look is taken into a project relating to supply chain management which is creating a Proof of Concept (PoC) for tracking shipments from a supplier to a manufacturing plant. The application to track the shipment and share information between different systems is added to a blockchain based on Hyperledger. The case study is conducted by interviewing a developer involved in the project.

6.3.1 Case description

The project aims to create an application to handle documents of shipments to and from its plants and to its stakeholders, the project focuses on sea freight. The existing process of document handling for supply chains is antiquated and requires a lot of paperwork. The large amount of documents lead to an error prone process, long handling times, and often no real time availability. While efforts are made to improve the document handling process using centralized systems managed by one of the stakeholders in the supply chain, often other stakeholders are hesitant to trust these systems. A DLT system offers a possible solution for this lack of trust between parties.

A proof of concept is being developed which can be used to handle the document stream of shipments in a supply chain. The current project aims at creating a minimal viable product, which is capable of tracking a shipment over sea. The application should comply with the following requirements:

1. Verification of documents legitimization and data ownership
2. Identification of possessive and negotiable documents
3. Real-time availability to all parties
4. Up-to-date data
5. Scalability

The interface with the blockchain is an online portal available to all stakeholders, which also connects to a number of existing systems. API calls to the vessel supplier reveals data on the shipment which is combined with data from the internal transport management system containing the contents of a shipment. For each shipment, a transaction is placed in the ledger with its transport number. Any document can be uploaded using the interface; this saves the document online and saves a hash, a pointer to the document, and a reference to the shipment to the blockchain ledger. When a stakeholder of a shipment wants to download a document, it is first checked for integrity using

the hash of the document and when this is verified a stakeholder can download it. The stakeholder is also able to add a changed document to the ledger, which will be available to all stakeholders.

6.3.2 Risk analysis based on preliminary model

Based on preliminary risk model, a number of areas for improvement have been identified. The project focuses on creating a minimal viable product, but design choices that are currently made can have a lasting effect on the rest of the project. The identified risks should therefor still be considered during development, even though the project is in an early stage of development.

The project is currently performed mainly within one organization, there are currently no external partners present in the ecosystem. The aim for the system is to involve other distribution partners as well but the status of this is currently unknown. The project needs to include more partners if it wants to create a functional product. Each partner should have benefits from using the system to encourage usage.

Any data can currently be uploaded into the system with a hash placed on the ledger. The files itself are stored on a centralized server of the organization. There is no filter or identification of files, which may lead to unwanted files uploaded to the system.

The DLT used for the system is Hyperledger Fabric, a large scale open source project. The code that is being written is difficult to test since smart contracts, named chain code on Hyperledger, need to be deployed in a new environment on each node for each update. With a small number of systems, this is still possible but it will become more difficult when the network will scale further.

There is not a large focus on speed of transactions of the system. This is because the system will be used only to record hashes of data. There have not been any tests for a larger number of transactions. Production level performance testing has not been performed.

6.3.3 Model fit

During the evaluation of the risks using interviews we found that not all identified risks were as relevant to the project than others. A number of risks were irrelevant due to the nature of the use case, other risks were less relevant due to the development stage of the project. The preliminary risk model has a number of risks that are focused on IoT, since the use case does not include any IoT devices, these risks are not applicable. Two other categories of risks that were found to be irrelevant because the functionality is not included in the use case are the risks relating to the areas of ‘External Data Sources’ and ‘Integration with Existing Systems.’ The external data sources risk focuses on connections made with external sources directly from the ledger, not via a separate cloud platform. The preliminary model does not have the possibility to adapt to specific use cases, it sees all DLT use cases as having the same possible risks.

Due to the status of the project, there were many aspects that are classified as risks in the preliminary model that have not been a focus yet during development. Risks regarding the governance of the application, while good to take into account during development, only become more important when the application is moved further towards a production system. According to the developer, the project is only a learning project and is not likely to move forward into production. While the risks may seem to be of less importance, they can be used to guide further development when a choice is made to continue towards a production application.

The preliminary model has no scaling available; a risk is either handled or not handled. For a number of risks in the model this simple identification of risks did not properly represent the state of the risk. The risks relating to code verification for example cannot be put into different categories.

While in the project code can be verified to be syntactically correct and working within one node, it cannot be tested and debugged on multiple nodes.

6.4 GS1 Palettenschein - Pallet deposit

The GS1 Germany, a standards organization, is leading a pilot project for tracking pallet deposits by multiple parties.[1] In total there are 29 companies involved in the project, one of which is Bosch. The application is currently being tested at a number of the participants. The goal of the project is to create a pilot application and not to launch a final product. After the pilot phase, a decision will be made to further develop the application or to discontinue the project.

6.4.1 Case description

The goal of the project is to create an application which can track deposits for pallets within the transport sector. These pallets are costly and therefor a bartering system is in place to keep track of the pallets changing hands between different parties. Within a two-party system with one supplier and one receiver it is easy to keep track of the deposit, within a multiparty system this becomes more difficult. Currently a barter system is used in which the players are not necessarily known and there are no standardized rules, rights and obligations for the exchange process. In addition, the exchange usually takes place bilaterally, without an intermediary instance such as an operator. In order to document the exchange processes, consignees use the bills as vouchers if the pallet exchange is not made directly. Most companies trade deposit vouchers and pallets with each other and in some cases via an intermediary. The owner can later redeem the pallet deposit himself or through service providers at the debtor. This process leads to much complexity and often times deposit notes are lost.

The Multichain blockchain protocol is used as a method to keep track of the pallet deposits without a central party that needs to be trusted. The main technical partner in the project is SAP which help to set up the blockchain. A web application is created by SAP to interact with the protocol. Participants of the project can log in here and record transactions that take place. When an exchange of pallets takes place, both participants involved in the exchange need to accept the transaction before it is written in the blockchain. Keeping track of the balance of participants is handled off-chain within a backend system from SAP.

6.4.2 Risk analysis based on preliminary model

This project is in a later stage of development with regards to the Twinflow project. A proof of concept has been created and a pilot application is currently being tested. With the current setup of the project the blockchain merely acts as a ledger to keep track of exchanges. These exchanges are not automated and no external legacy systems are involved. It may be possible that in a next stage of the project these aspects will become relevant.

The assessment of the project based on the preliminary model showed a number of areas where the project can be improved. These risks also correspond to the notes made by the developer. A big area which still needs improvement is the governance area. Risks relating to change management and identity access management are not properly handled yet. The system is currently mostly built by the technical partner SAP, a governance structure to handle software changes after the project is

[1] More information: https://www.gs1-germany.de/innovation/trendforschung/blockchain/pilot/

not available yet. Participants of the pilot study have access to the system but a method to handle access controls after the pilot project is also not available yet.

Currently the performance of the application is not measured. The overall performance is tested through a number of pilot studies but the scalability of the system is not tested. While the speed of a transaction is currently not the focus of the project, it can become an issue when the network is scaled up.

Data within the transactions are open for all participants to see. While this was brought up by some of the participants in the system, it is needed for the architecture of this system to function properly. It might be possible to reveal business critical data from other participants when analyzing their transactions.

Regulatory compliance of the project is most likely to be handled through clauses in physical contracts between participants. Within these contracts, clauses will be included to prevent participants from uploading private or illegal data to the blockchain. While this does provide some assurance, it might still be possible for illegal data to be put into the blockchain. Furthermore, no extensive analysis has been done yet within the project to identify other relevant legislation .

6.4.3 Model fit

From the aspect of functionality of the application, the model suffers the same issues as with the previous use case. There is no IoT functionality yet and this has not been a focus of the project. Furthermore, there is no connection directly from within the ledger to other data sources using Oracles or to any legacy systems.

The DLT platform choice sub risk was not directly relevant to the use case. The criteria depend on the requirements of the use case and, in this case, smart contract capabilities and IoT specific fic are not directly relevant.

6.5 Share&Charge - EV charging

eMobilify is creating a protocol, the Share&Charge protocol, which supports the interoperability of Electronic vehicles and charge points. This will help owners of electric vehicles to overcome the hassle of dealing different charge point providers which have different systems which do not work together well. It is part of a larger project which aims to eventually create a fully decentralized solution of charging electronic vehicles.

6.5.1 Case description

eMobilify has been working on the Share&Charge project already for longer period of time. Their first production ready system was launched in April of 2017 which build upon existing charge point infrastructure using the Ethereum protocol. During the production run of the system they encountered a number of issues which led to the choice to shut down the application in 2018. In order to tackle the issues encountered, they decided to start working on building their own infrastructure for an Electric Vehicle (EV) charging network.

The goal of the project is to create a system in which EVs and charge-poles interact directly with each other through a DLT network. They aim to achieve this vision through a number of stages, after each stage the system becomes more decentralized. The first step is to create a system that builds on top of the existing infrastructure but talks directly to the Charge Point Operator (CPO) and Mobility

Service Provider (MSP). This allows for a more gradual integration and a smaller step for existing providers while still providing some of the benefits of a decentralized solution.

In the first stage, eMobilify provides a number of services in collaboration with its partners; it creates a smart contract including the business logic of charging, it provides a client to connect to the blockchain for a CPO and it provides wallets for MSPs to pay for charging the EV. It builds on top of an existing blockchain network for energy providers named the Energy Web Blockchain (Energy Web Foundation, 2018). The architecture is visualized in figure 6.1.

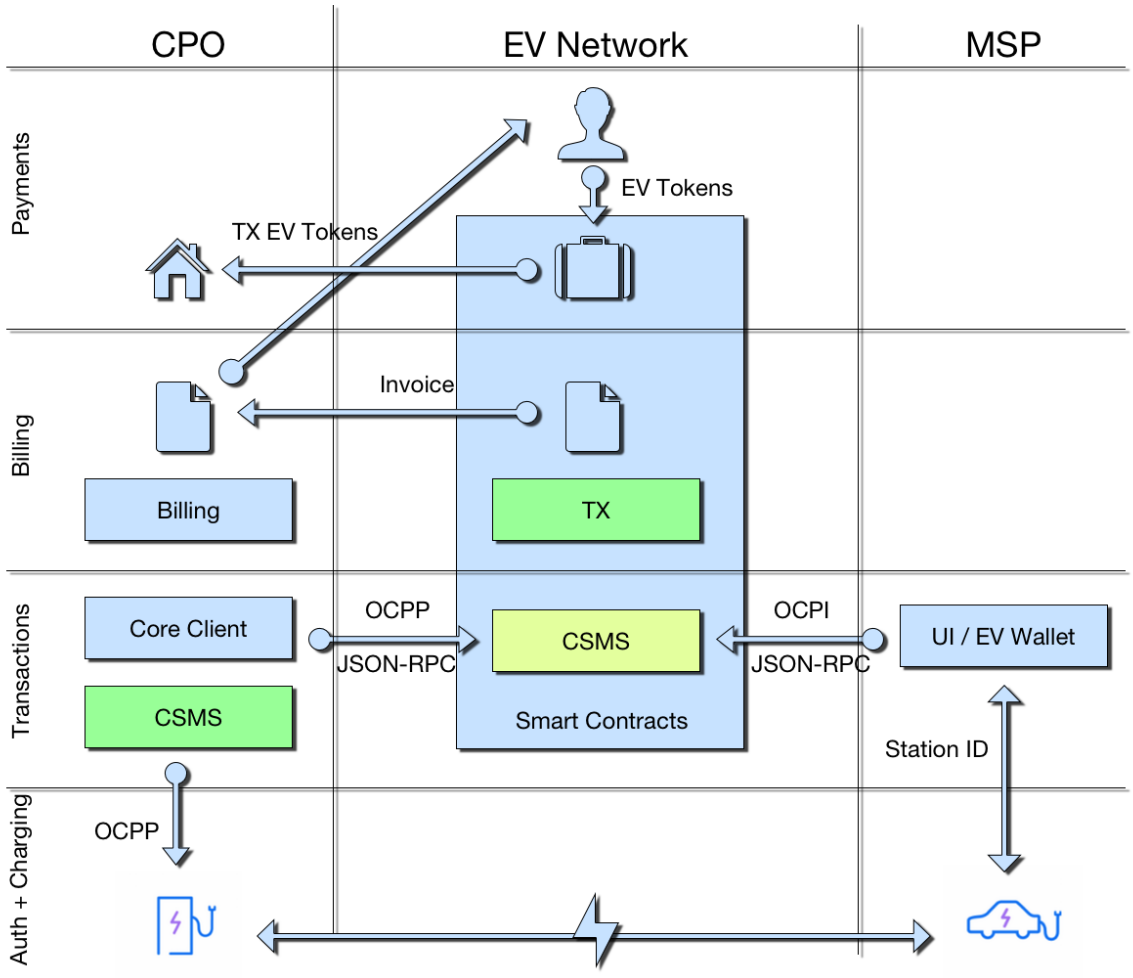

Figure 6.1: Share&Charge architecture (Garcia, 2018)

6.5.2 Risk analysis based on preliminary model

This risk analysis focuses on the current state of the project. It is currently in a pilot stage where the current architecture is tested, the results of this pilot are not yet known. The model has identified a number of risk areas which still need further attention before the application should go into production. Many of the risks are similar to areas where eMobilify is still working on improving their product.

The project works together with multiple parties which all have to work with the same smart contract. It may be possible that at some point attributes of this contract should be updated. There is currently no governance structure set up to have influence in the decision process of updating aspects of the contract. This may become an issue if there are participants which have conflicting ideas on how to update the contract.

GDPR may form a problem to the network but it is not sure yet how legislation will handle this technology. There is no data open for anyone to see but it may be possible that hashes are also seen as personally identifiable data. If this is the case the architecture of the system should be adapted.

Banking regulations, for example KYC and AML regulations, should also be taken into account since there is an exchange of value tokens that are used for payment. There has been an evaluation of the banking regulations but the design of the token is not final yet. When the design of the token is changed other regulations may be applicable.

The current set-up of the project using an Ethereum network does not provide some of the support needed for nodes to run on IoT devices. While in the current architecture there is no need for the clients to run on these IoT devices, the vision of the project is to move the clients to IoT devices. They are waiting for the overall ecosystem to develop further and provide a good solution for connecting IoT devices straight to a blockchain.

The network on which the system is built is not production ready yet. It is still in development with only a testnetwork available. Not all functionality of the chain is functioning properly yet. A projected launch of a production chain is in Q3 of 2019, but there are no guarantees in place. If the network does not live up to its promises the Share&Charge project will have to adapt their application.

6.5.3 Model fit

Evaluating the Share&Charge project with the model brought forward a number of insights into the model. It is focused on a single application working with DLT. This project includes a multitude of applications with different functionalities and different risk profiles. Certain aspects of the model, like integration with existing systems, is different for each application. This was solved in the case study by evaluating all the different aspects and basing the risk on the application with the highest impact risk. This was chosen since the risks of the entire system relies on the most vulnerable part of its individual components.

It was also found that a risk was missing from the model relating to the category of DLT protocol choice. There is no risk that evaluates what kind of permission protocol for accessing and writing to the blockchain is supported by the protocol.

6.6 Odometer fraud

Odometer fraud is a common way of increasing the value of a car by manipulating the mileage. When you buy a second hand car, mileage is one of the key components determining the value of a car. With the shift from manual to digital tracking of mileage came also a shift in methods to manipulate mileage. For many cars with digital odometers it is possible to manipulate the mileage by simply connecting your car to a specialized tool which reverts mileage data. In order to create more trust in the digital odometers blockchain technology is used to immutably store historical mileage data.

6.6.1 Case description

The project aims at creating a record of historical mileage data of cars. Using a telematics service built-in to the car or retrofitted, mileage data is collected and uploaded to a cloud which puts it in the blockchain. Within a mobile application the user has control over the data which is produced by the device. The user can decide how often the mileage data should be uploaded and can read previous readings of the meter.

The meter in the car sends the mileage data to a node running outside of the car in a cloud service. This node pushes the hash of the mileage data into a bitcoin network to ensure the immutability of the data. A merkle path of all the hashes collected by the meter is saved on an external database outside of the bitcoin network.

6.6.2 Risk analysis based on preliminary model

The project with odometer fraud is in a late stage of development with a product almost reaching the market. Even though this is the case, a couple of risks have been identified which may have an impact on the application. Some of these risks do not form a big threat to the application while others form a larger issue.

The data is being collected using a device which uploads it into the blockchain. There are a number of steps involved before it is uploaded into the blockchain and it is possible for the data to be manipulated before it reaches the blockchain. While it reduces the chances of odometer fraud, it does not eliminate it.

The blockchain that is used, Bitcoin, is not a good fit for IoT devices when using the device as a node. While with the current set-up this is not an issue, direct IoT integration with smart contracts is a possible way to upgrade the system to make it more secure against manipulation.

The system is currently run within the servers of one company, there are a number of distribution partners available but they are not part of the network. While this reduces the risks of one participant dropping out of the network, it centralizes the system and introduces more of the risks apparent to traditional databases.

6.6.3 Model fit

The model identified a number of areas where risks could occur. Some of these risks apply to the current state of the application but many can be identified for a possible future state of the application. When choosing to only look at the current state of the application a number of the identified risks are not relevant. A choice should be made to either evaluate only the current state of the application or to also look at a possible future state. When a choice is made to only look at the current state, a number of risk areas should be adapted to better identify risks relevant to this type of use case. This can include altering descriptions of the risks to also identify partnership risks in other parts of collaboration besides only within the DLT network.

6.7 Groningse Kredietbank - Debt relief

The Grongingse Kredietbank (GKB) supports debtors in getting out of their debts by offering services like courses and small loans. Keeping track of all the documents relating to the debtor is often a difficult task for the GKB. It may be possible that certain documents go missing or mistakes in filing are made. In order to create a better overview for the debtor and the GKB, a system is proposed to collect the related documents for the debtor and the GKB and keep the debtor in control of its own data.

6.7.1 Case description

In order to better support its clients in managing their debts, the GKB have started a project together with CGI in which data relating to its clients is managed in a blockchain. A successful proof of concept

was created and is being further developed into a production ready system to be used by the GKB.

The application that is being developed consists of a dashboard for debtors and GKB employees. Entities that want to collect debt from the debtor can check if the debtor is registered at the GKB and submit their request for payment through a portal. This way a collector of debt does not unnecessarily start a claim against a debtor who is unable to pay.

All information is stored on an Ethereum permissioned blockchain running on nodes owned by the GKB and parties which have a direct connection to the system to upload claims to debtors. Each party with claims is able to upload their claims to the system which then stores it in a separate cloud with the hash in the blockchain. Only the debtor, the GKB and the debt collector are able to access the documents.

6.7.2 Risk analysis based on preliminary model

Based on the preliminary model a number of risks were identified within the project. The first one is the choice to run a system on the blockchain. Upon an analysis the conclusion can be drawn that the blockchain may not be the most efficient back end for the system. Due to all of the centralization tendencies of the system, a traditional database may also be used to create a system with similar functionalities.

Currently the system is limited to the municipality of Groningen. The full benefits of the system can only be established when more municipalities and debt collectors are involved in the system. Since the system requires a custom connection to existing systems, it may be difficult to involve more parties in the system because of the extra processes involved and relatively high startup costs.

The performance of the system is currently not a bottleneck since there is no large scale deployement of the system yet. Due to some of the restrictions of the Ethereum blockchain adding data to the system may take up to 15 seconds per record. When scaling up the system this may become an issue.

The development of the system started with a proof of concept formed out of a simple project from a Hackaton. Some of the choices made early in the project create limitations for the current state of the project. These decisions made earlier in the project are not being revised because of costs reasons. This may create a system with legacy code which does not function properly.

6.7.3 Model fit

During the last use case evaluation some earlier identified shortcomings of the model were further confirmed. In this use case there is no IoT involved and there is no plan for there to be. The governance structure of the application is not fully set up yet but it will likely consist of a centralized structure. There is currently no risk which solely focuses on the risks relating to a centralized governance structure of a decentralized application. A truly decentralized application should also be governed using a decentralized governance structure. The risks relating to a centralized governance structure should be better emphasized in the model.

Overall the model fit well with the use case. Many of the risks which were identified in the model were also identified in the use case. Not all risks were handled and many were only partly handled. This also calls for a more staged approach for the model. The risk relating to GDPR compliance shows this well: while there has been a big focus on making the application GDPR compliant and they believe they have, there has not been a ruling yet which makes it clear how the regulation will be applied to blockchain application.

6.8 Conclusion

The preliminary model was able to identify a large number of risks relevant for the use cases. A limitation of the current form of the model is that the level of the risk cannot be consistently identified. While in one use case an effort may be made to reduce the impact of a risk, it will rate the same as an application where no effort is made to reduce the impact. In order to compare these cases, a model which include pre-defined levels will be more beneficial.

Between the different case studies we have also identified a number of areas where the model may not fit well with the analyzed use cases. Elements like IoT fit of a DLT protocol and external connections are not relevant for use cases where these elements are not included in the application design. While for some use cases these elements may become relevant in a future state of the application, for others they will stay irrelevant.

When applying the risks from the different risk areas we found that a number of sub-risk areas were either overlapping or did not fit well with the use cases. These areas are programmer expertise and skill, code ownership, external data sources and DLT platform partners. The risks from these areas have been moved to other sub-risk areas. The ‘programmer expertise and skill’ sub risk area overlaps with the ‘code quality risk area’, as the risks of programmer expertise is often poor code quality. ‘Code ownership’ overlaps with ‘legal liability’ due to the agreements formed with code ownership. The ‘external data sources’ sub risk area has been combined with the ‘integration with existing systems’ sub risk area since we decided to limit our scope only to the security of the DLT and not all the external systems connected to it. The ‘DLT platform partners’ sub risk area can be combined with the ‘DLT platform choice’ risk area. Since within the choice of a DLT platform, the functionality of the platform should be investigated but also the partnership risks of using the platform.

The model may not be as useful to analyze developing proof of concept applications. These applications have a lot of risks associated with them but they merely exist to show the possibility of a concept for an application. Many design choices are made based on ease of development and while these design choices may form additional risks, this may not be relevant since the proof of concept will not be further developed. When a choice is made to further develop the application into a production system, the risks become relevant.

Based on the findings from the use cases it can be concluded that the current model is not a good fit for all applications. The model needs to be further generalized, or a restriction should be made as to what applications can be measured using the model.

Chapter 7

Forming the maturity model

The risks that have been identified through the Delphi study and tested with the case studies are translated into a number of level descriptions in order to create a maturity model which can be applied to specific DLT use cases.

7.1 Focus of the model

Based on the findings during the case study the focus of the maturity model has been narrowed. As further explained in the previous chapter, the risks did not properly match with the varying use cases. This was mainly due to the varying methods of using DLT and the different business environments DLT can be used in. In order to create a model which can better identify risks for a DLT application, a number of criteria for the use case are identified. A DLT use case which adheres to these criteria can be properly analyzed using the maturity model.

The case studies have shown that the risks fit a number of use cases better than others. We have decided to create the criteria for the model based on the best fitting use cases and generalize from these cases. The criteria of the model are based on the case study of the project from MotionWerk regarding a smart charging system. This use case has been chosen because the application shows a clear maturation path through it's different iterations of the system and a possibility to connect IoT devices directly to the chain. The criteria for DLT applications are the following:

- IoT devices should be used currently or in the near future within the DLT application.
- DLT application is benefited by higher transaction speeds.
- DLT application is created by a business and used for B2B or B2C interactions.

7.2 Level descriptions

The level descriptions specify the maturation path for each of the sub-risk areas. The descriptions will form the basis of the maturity model. The maturity paths are based on the results of the Delphi study, case study findings and existing scientific literature. Where there were knowledge gaps, field experts were consulted to help create the descriptions.

In order to be able to compare the maturity of varying areas with each other, the overall maturity levels have been identified based on the CMMI level descriptions (CMMI Product Team, 2010). They have been adapted to better fit our purpose:

Level 1. Ad hoc - No processes to handle the identified risks. Risks are not consistently addressed only and on an informal basis.

Level 2. Initial - Processes are in place to handle risks but they are not standardized. Often times risks are mitigated after the risk has taken place.

Level 3. Repeatable - Processes are characterized to handle identified risks and are standardized. Processes are proactive in identifying and mitigating the risks.

Level 4. Managed - Processes in place to control the identified risks based on continuous measurement and control

Level 5. Optimizing - Continuously looking for possibilities to improve processes of mitigating the identified risks.

7.2.1 Strategic area

Within the strategic risk area, two underlying sub-risk areas have been defined. These are DLT platform choice and DLT ecosystem partners. The overall definition of the strategic risk area is the following:

> *Risks arising from strategic decisions surrounding the choice for a DLT and the partners in the network.*

DLT platform choice

There are many different platforms available which can be classified as DLT, each with their own capabilities and limitations. When a DLT application is developed, the platform that is used for development should be carefully chosen since it can cause limitations later on in development. In order to evaluate the basic fit of a DLT platform to a use case one should perform an in depth analysis of the platform and compare it with other available platforms. The criteria below are a number of criteria that can be taken into account when choosing a DLT platform:

- IoT specific fit

  An analysis should be done in order to assess how the platform can run within the restrictions of many IoT devices. The restrictions that should be included in this analysis are: Limited bandwidth, Limited battery power, Limited storage, Limited processing power

- Data structure

  The data structure that is being used in the DLT (i.e. blockchain, DAG, combination, etc.) should be considered if its fitting with the use case, taking its limitations into account. For example, scalability issues with blockchain and issues with incentivizing in DAG. Furthermore, the most fitting data structure depends on the data that is being shared and the requirements of this type of data. It may need to move over the network quickly or it may need to be a large amount of data, which does not matter if it takes long to complete the transaction.

- Smart contract capabilities

  The type of smart contracts that can be performed with the platform must be taken into account when deciding which platform to choose. Aspects that should be taken into account when looking at smart contract capabilites: Turing completeness, code performed by every node, sharding mechanism, calling other contracts, calling external sources.

- Consensus mechanism

  The type of consensus mechanism which is being used for the platform should match the requirements of the business case. Aspects that should be taken into account when selecting a consensus mechanism: Amount trust in other participants, Hardware capabilities, Amount of decentralization, Transaction finish time (speed of consensus), Attack vectors (Sybil attacks, 51% attack, selfish mining, and others).

This sub-risk area focuses on making sure the correct platform for the use case is chosen. The following maturity levels evaluate how the choice for a DLT platform have been made. The criteria described above can be seen as a guideline for choosing a DLT platform.

Level 1. Platform is chosen based on availability of technology or developmental experience of developers. There has been a basic analysis for fit for the use case based on experience of developers.

Level 2. Requirement analysis for the use case has been performed to analyze the fit for the use case.

Level 3. Pre-defined criteria are in place to measure fit of a platform to a use case.

Level 4. Recurring comparative analysis is in place to evaluate the platform throughout it's lifetime.

Level 5. Possibility to easily switch or alter platform when a better suiting platform has been identified.

DLT ecosystem partners

The DLT ecosystem partners sub risks focuses on the risks that arise from working together with other partners. Within a DLT ecosystem this brings along some specific risks additional to traditional risks of collaboration. When evaluating the maturity of partners these traditional risks such as liability or information oversharing (Merchant, 2011) should be taken into consideration but are outside of the scope of this model. The two main risks which have been identified in this area are the following:

- Critical mass of participants not reached
- Network participant pulls out

Alonso, Martínez de Soria, Orue-Echevarria, and Vergara (2010) have created a maturity model for enterprise collaboration which closely relates to the challenges with DLT ecosystem partners. Elements from this model are adapted and combined with the identified risks to form the maturity levels for this risk area.

Level 1. The application is only run internally in a closed environment without partners.

Level 2. The application is run within a consortium of businesses with each participant performing a single unique function in the network. When one participant decides to stop using the system the network will lose functionality.

Level 3. The application is run within a consortium of businesses with multiple participants performing similar functions within the network. A small part of consortium contributes to improving the network. Agreements are in place with ecosystems partners to ensure participants stay in the network.

Level 4. When one participant decides to stop using the system, a different participant can offer similar functionality. Partners are actively recruited.

Level 5. Each participant is actively managing and improving the network. Partners are actively joining network due to market leadership.

7.2.2 Operational

Within the operational risk area, three underlying sub-risk areas have been defined. These are DLT performance, data management and change management. The overall definition of the operational risk area is the following:

> *Risks arising from inadequate or failed processes, people or systems surrounding the DLT application.*

DLT application performance

The DLT performance sub-risk pertains to the performance of the DLT protocol as used by the application. Performance not related to the DLT, such as write speed to a cloud storage, is not included in this category.

To evaluate the performance of the DLT application a number of metrics need to be defined. These should guide the performance evaluation and create common definitions across different DLT protocols. Adulla et al. (2018) have been working on establishing these common metrics and have identified four key metrics, which are summarized below. For a more complete report on the performance metrics we refer to their white paper.

- Read Latency

  Read latency is the time between when the read request is submitted and when the reply is received.

- Read Throughput

  Read throughput is a measure of how many read operations are completed in a defined time period, expressed as reads per second.

- Transaction Latency

  Transaction latency is a network-wide view of the amount of time taken for a transactions effect to be usable across the network.

- Transaction Throughput

  Transaction throughput is the rate at which valid transactions are committed by the blockchain in a defined time period. This rate is expressed as transactions per second at a network size.

In order to create maturity levels for this area, mitigation strategies of performance risks are taken a look at. Gupta (Gupta, 2014) proposes a number of mitigation strategies regarding speed related performance risks. These have been customized to fit more closely to DLT related performance as established above. In order to measure the system, the above mentioned metrics should be used.

Level 1. Simple usability tests are performed on the application and a small scale qualitative performance tests are performed.

Level 2. Performance of application has been tested once quantitatively using key metrics with production-like circumstances.

Level 3. Periodic testing of performance and processes are in place to modify resources in order to increase performance.

Level 4. Continuous measurement of application performance with notification when performance falls under specified minimum.

Level 5. Continuously optimizing DLT application performance. Automatic response when performance falls under specified minimum.

Data management

The data management sub-risk area focuses on the process of adding new data to an immutable DLT. Integrity of data can easily be verified with a DLT, but verifying the cannot inherently be done with a DLT. Due to the decentralized nature of DLT there are many participants adding data to the ledger and gaining assurances of accuracy of the added data can prove to be difficult. While the need for accurate data may differ depending on the use case, one should strive to include as much as possible accurate data in the ledger.

In order to define the maturity levels for this sub-risk area, existing maturity models regarding data management and data quality management are used. In the field of data management there are already a number of maturity models in place. Models like the CMMI Data Management Model (CMMI Institute, 2014) encapsulate the entirety of data management, from data governance to data quality, while other models like the Corporate Data Quality Maturity Model (Hüner, Ofner, & Otto, 2009) focus only on the specific domain of data quality management. The data management sub-risk area as defined within this model, relates closely to the domain of data quality management. The aim of the sub-risk area is to identify the correctness of the data that is being onboarded onto the DLT and to make sure no illegal information is added to the DLT.

Level 1. Data that is already in the ledger is assumed to be accurate and no procedures are in place to verify accuracy. All data is able to be added to the ledger.

Level 2. After an incident relating to inaccurate data in the chain takes place, the accuracy of data is checked according to procedures which are previously defined and documented for data inspection. Procedures are in place to identify illegal data before it is added to the ledger.

Level 3. Data onboarding procedures are in place for all data providers to ensure data accuracy. Accuracy of provided data is auditable by other participants. Illegal data are being automatically barred by a front end from being onboarded onto the ledger.

Level 4. A monitoring system is in place to automatically verify data accuracy, when data is not accurate it is not allowed on the ledger.

Level 5. All added data on the ledger is accurate and auditable. Procedures to remove or block private or illegal data are in place without losing the integrity of data on the ledger.

Change management

Change management in this sub-risk area is defined as the management of software changes by participants of the DLT. These are changes both to the application and the protocol used. Depending on the type of application and the type of DLT used, participants can change a number of aspects of the software. When a disagreement is formed it is possible that this causes a split in the network, called a fork, where one part of the network accepts a change and another part does not.

Applications running on the DLT may be more easily changeable depending on how the application makes use of the DLT. If it only writes and reads transactions to the DLT the change can be made on the application side to write and read different data formats. In the case that smart contracts or other executable code is used on the DLT it may be more difficult since the contracts need to be updated. Research is being conducted to create secure updatable contracts (Bloo, 2018), but currently the best method to update is to write a new contract if possible.

The main risks as identified in the previous round, a lack of consensus on upgrades of the DLT and the creation of multiple truths due to forking. Both of these risks can be mitigated using a well-founded governance structure to decide over changes to the network.

Level 1. Changes to application running on DLT are made ad-hoc by central authority with little collaboration with ecosystem partners.

Level 2. Process in place for ecosystem partners to challenge changes proposed by central authority.

Level 3. Governance structure in place to handle changes to the application with one central authority but the possibility for ecosystem partners to suggest changes.

Level 4. Governance structure in place with small consortium who decide on changes to the application.

Level 5. Open governance structure with all entities able to contribute code and balanced voting power distributed over all participants.

7.2.3 Security

Within the security risk area, 4 underlying sub-risk areas have been defined. The overall definition of the security risk area is the following:

Risks arising from security incidents surrounding the DLT and IoT devices.

Endpoint security

The DLT network is only as secure as the endpoints which interface with the network. While network tampering by a certain amount of malicious nodes is often mitigated by the network, it can become an issue if the number of malicious nodes increase. This sub-risk area looks at risks relating to the endpoint security with a focus on IoT devices. These devices often have limited capabilities and are not well secured. There are a large number of attack vectors on IoT devices which must be taken into account (Khan & Salah, 2018). While a complete analysis of these attack vectors is outside of the scope of this research, the security of these devices needs to be considered when allowing them to be part of a DLT network.

In order to create the maturity levels for this sub-risk area the level descriptions of the IoT Security Maturity Model (Carielli, Rudina, Soroush, & Zahevi, 2018) are used in combination with the risks as identified in this research. The risks in this area are related to risks with IoT devices on which the ecosystem has control. If an open network is chosen on which any IoT device is able to join, no guarantees can be given with respect to the security of the network.

Level 1. Reliance on inherent DLT characteristics to protect network from malicious nodes in the network.

Level 2. Requirements for devices are distributed to providers of IoT devices that participate in network which cover main use cases and well-known security incidents in similar environments.

Level 3. Permissioned network with extended security requirements for devices which are based on best practice, standards, regulations and classifications, is in place. Devices are checked to identify if they comply with the required security characteristics before they are allowed to join the network.

Level 4. Network with automatic access restrictions when joining based on dynamic adaptable security framework tendered to resource limitations of device.

Level 5. Measures are in place to detect and restrict access to malicious devices based on usage patterns of the device.

DLT protocol attacks

This sub-risk area looks at technology risks relating to the consensus mechanism or other parts of the DLT protocol being abused. This area looks at how well the risks of the chosen DLT protocol are identified and handled. The risks of the different protocols vary greatly depending on the type of consensus mechanism used, types of smart contracts, and other factors.

For the chosen DLT platform with which the DLT application interacts, the possible technology risks which should be investigated and measures should be taken to reduce these risks. While DLT is well protected against malicious participants in the network, it is still possible for the integrity of the network to be impacted by a number of attacks.

- 51% attack
- Sybil attack
- Selfish mining attack
- Double spend attack
- Majority of nodes lost
- Centralization of nodes

It is often not possible to completely protect against these types of attacks. A number of methods do exist in order to reduce the chance of an attack impacting the network. For each DLT platform the risks are different and therefore there is not one general solution possible for protection. The maturity levels from this sub-risk area are based on the maturity model for IT Risks defined by ISACA (2009).

Level 1. Episodic risk assessment performed based on minimal understanding of related DLT protocol risks. No processes in place to mitigate risks.

Level 2. Analysis performed based on select known security risks. Worst-case scenarios are focus. Periodic assessment of risks and mitigation strategies defined.

Level 3. Extensive analysis on possible security risks performed. Amount of accepted risks defined. Mitigation strategies in place to reach the accepted risks.

Level 4. Automatic detection of risks based on defined DLT protocol risks. Mitigation strategies defined or adapted when risk is identified.

Level 5. Automatic detection of security risks and improvement of detection based on learning algorithm. Mitigation automatically adapted to reach desired acceptance of risks.

Identity management

On many DLT networks, the identity of participants is reliant on private keys. Access can be restricted using these keys or the network can be open to all keys. When a private key is lost or stolen, they can often times not be restored. Furthermore, the key can be used to imitate other participants in the network to perform malicious actions.

This risk area focuses on risks relating to the management of keys relevant for the DLT application. There are a number of methods available to reduce the risk of key loss or compromise. Depending on the type of keys that are stored, different methods of storing could be most suitable. Often times the most secure methods of storing a key are the least convenient. A balance must be struck between security and convenience.

There are a number of methods available which help reduce the chances of losing a key or reduce the impact when a key is lost. These methods can be used as a guideline to improve key storage security but should be further researched.

- Cold storage of keys
- Layered security to access keys
- Eliminating single points of failure
- Hardware Security Modules (HSMs) to generate and store keys
- Multi-signature access to network and smart contracts
- Monitoring anomalies in network and key storage
- Processes in place which help reduce the risk of key compromise

This sub-risk area closely relates to the identity and access management field which is well established in the information systems field with a number of maturity models available (Gartner, 2018a; Kuppinger, 2007). These models are used in combination with the risks and use case studies to create the following maturity levels.

Level 1. Single points of failure in key storage evident. Keys are created ad-hoc and not stored in a consistent method.

Level 2. Key management system is available to store keys and give access to individuals. Policies defined to create and gain access to keys defined per project.

Level 3. Policies in place to proactively reduce risks of stolen and lost keys with methods like key rotation. Storage and creation of keys through hardware security modules.

Level 4. Monitoring anomalies in network and key management system in order to identify possible instances of malicious use of keys. Processes in place to revoke keys.

Level 5. Continuous improvement of key management policies.

Transaction security

The transaction security sub-risk area focuses on the security of the information stored within transactions and smart contracts. Depending on the type of network, the information stored within transactions can be viewed by other parties who are not involved in the transaction. In addition, the metadata of the transaction can be used to deduce information which may be sensitive, such as some critical business processes of a competing company (Christidis & Devetsikiotis, 2016).

The amount of sensitive information on the chain should be limited, but when it is necessary to include this information it should be properly secured. There are a number of methods to reduce the chance of information being gathered from the content or metadata of transactions. Depending on the use case these methods can be applied on application or DLT network level.

- Homomorphic encryption

  Using Homomorphic encryption, elements of the transaction can be kept secure while still allowing for operations to be executed on the transaction. This method has not been established yet in DLT but an alpha version of Elements has this form of encryption available (Maxwell, n.d.).

- Zero-knowledge proofs

  Zero-knowledge proofs allow for one party to prove to another party the validity of a statement without revealing its content. This method is currently being tested in the Hawk project (Kosba, Miller, Shi, Wen, & Papamanthou, 2016).

- Mixing protocols

  Mixing protocols can be used to further anonymize individuals on the blockchain. Current research in this area is mostly focused on the Bitcoin blockchain but it may also be applied to different DLTs in order to reduce the information that can be deduced from metadata (Conoscenti, Vetro, & De Martin, 2016).

This area focuses on information stored on a public or permissioned chain on which the participants on the network do not fully trust each other and therefore do not want to have sensitive information within transactions revealed.

Level 1. Transactions are open for other participants in the network to view and no processes are in place to ensure no sensitive data is added to the ledger.

Level 2. Per transaction there is a manual process to ensure no sensitive data is added to the chain. Sensitive data is not clearly defined.

Level 3. There is an automatic process to ensure no sensitive data is added to the ledger. There is a clear definition for data which may and may not be added to the ledger.

Level 4. Measures are taken in order to reduce the possibility of information to be gathered from the contents or metadata of transactions.

Level 5. Continuous improvement of transactional security mechanisms including auditing testing of mechanisms to ensure security.

7.2.4 Legal

Within the Legal risk area, 4 underlying sub-risk areas have been defined. The overall definition of the legal risk area is the following:

Risks arising from legal challenges surrounding the DLT application.

Regulatory compliance

The regulatory compliance sub-risk area looks at the processes relating to the compliance of the application with applicable regulation. Depending on the use case there are a number of different regulations to take into account. From an IoT aspect the most common regulation that is currently debated is privacy regulation like the GDPR (Finck, 2017). When there is an exchange of fiat to digital currency it is likely that KYC and AML regulation will apply (Larsson, 2018).

The current landscape of legislation around DLT is not established yet as regulators are struggling with handling the new nature of the technology. It is possible that new legislation comes into play that

makes existing DLT solutions non-compliant. In order to reduce the chances of this happening a legislative outlook should be performed to see if there is a likelihood that relevant legislation might change in the future.

- General Data Protection Regulation (GDPR)

  The GDPR regulation is applicable to any system that handles any information relating to an identified or identifiable natural person. A number of aspects cause there to be much unclear about how to be compliant with the GDPR. One of the aspects relating to DLT systems which is still unclear is if hashed personal information is also considered identifiable information. There has not been a ruling yet which can be used to establish what is compliant. The articles which relate most to DLT are articles 17 and 25 (Finck, 2017). These articles handle the ”Right to Erasure” and ”Data Protection by Design and by Default” respectively. These articles seem to conflict most with DLT solutions as they are immutable by design and transactions are traceable in some form to an individual user of which the identity may be known or unknown.

- Know Your Customer (KYC) and Anti-Money Laundering (AML)

  KYC and AML legislation relate to customer identification in order to reduce money laundering activities. When there is a value exchange between fiat and digital currency it is likely that these regulations need to be considered. Recently, a new directive from the EU replacing older AML legislation creates a more clear outlook on how virtual currencies are handled under the European AML legislation (Directive (EU) 2018/843) (Larsson, 2018).

A number of existing regulatory and corporate compliance maturity models which have been used to create the maturity levels for this sub-risk area. RSA has created a maturity model relating to regulatory and corporate compliance management (RSA, 2018). Elements from this model have been used to create the maturity levels for this sub risk area.

Level 1. No formal evaluation of compliance with legislation is performed. Evaluations that are performed are inconsistently applied, informal and incomplete.

Level 2. Evaluation of compliance is performed after development of the application. There are some compliance controls in place but they are not integrated into the overall compliance management of the organization.

Level 3. Compliance with regulation is taken into account during the development of the application. Compliance controls integrated and standardized across the organization.

Level 4. Legislative outlook is performed to evaluate compliance with possible future regulations. Periodic reviews are conducted to assess the effectiveness and completeness of the compliance controls.

Level 5. Regular review and feedback are used to ensure continuous improvement towards optimization of compliance processes.

Legal liability

Legal liability is an important aspect when creating a DLT network or joining an existing network. It is a complex topic where the results of the liability may differ depending on the jurisdiction. Overall it can be asserted that DLT, public or private, are not beyond the law’s reach and participants can be held accountable for their actions. For an extensive analysis of legal liability of DLT we refer to

(Zetzsche, Buckley, & Arner, 2017). This section is based on the assertions made in the referenced paper.

This sub-risk area looks into the liability of an entity participating in a DLT network and applies to both public and permissioned networks. We look at liability among the ledgers (i.e. internal network liability) and liability to third parties (i.e. external network liability). This section will explain what types of liability can be applicable to participants of a DLT. With liability claims four different approaches can be taken. Which type of liability will arise will depend on the details of the DLT system, in particular the consensus mechanism, and on the rules of the specific applicable legal system or systems.

- Contract

  In order to establish liability, a contract and a breach of the contract are required. Contractual agreement requires an offer and acceptance (to establish mutual assent), consideration (anything of value exchanged) and an intention to create legal relations. While in cases with physical agreements or contracts in place between participants this liability is clear, in other cases a contractual agreement is not directly clear but it can be argued it is existent. For instance the fact that nodes participate in the system knowing that third parties will rely upon it, may turn their participation in the distributed ledger into legally consequential conduct.

  To establish a breach of contract general principles of contract law apply: Whether a term is a condition or a warranty depends on the intentions of the party discerned from the contract in light of context. Therefor a term does not have to be explicitly stated in a physical contract. For contractual liability, it makes no difference whether the damage resulted from the misconduct of a human being or a machines malfunction. The owner or operator is liable for the machines malfunction.

- Tort

  Tort claims could arise from damages to property via the distributed ledger. An entity operating in the distributed ledger may be liable in tort if its negligent act, omission or misstatement causes loss or damage, including loss due to a security breach or a coding error. An entitys liability in negligence will depend on whether it owes a duty of care and has breached that duty, whether the breach caused loss or damage, and whether it has effectively contractually excluded liability for this type of loss or damage.

  The existence of a duty of care depends in part on the type of loss suffered and by whom it is suffered. The relevant operator might establish that no duty of care existed, particularly if the plaintiff is a second or third line victim and not part of an ascertainable class. Liability for pure economic loss is therefore more likely in the case of smaller, permissioned blockchains where the class of plaintiffs is readily ascertainable, although the plaintiff would still need to prove the entity breached its duty of care and that this breach caused the plaintiffs loss.

- Partnership or joint liability

  If a cooperation is a partnership it will usually result in joint liability. In order to establish liability, first a partnership or joint venture needs to be established. While under the laws of some jurisdictions the joint pursuit of a (joint) objective suffices to establish an unincorporated company, the law of most common law jurisdictions require for a general partnership the sharing of profits. While participation in a clearing and settlement distributed ledger system that relies on all nodes mutual cooperation for identifying true transactions may be deemed a joint pursuit of a shared objective sufficient under some civil laws to establish a joint venture, the fee and profit sharing agreement will determine whether such a blockchain is deemed a partnership

under common law. With a partnership established, an entire network can be deemed liable for damages against a third party.

- Specific regulation

  Specific regulation may pose risks if DLT functions as a technological barrier that enables or facilitates monopolies. The additional liability may stem from competition / antitrust law. Participants involved in a distributed ledger system must keep this and other conduct-related legislation into account. This liability coincides with the Regulatory compliance sub-risk area and is not be further investigated in this sub-risk area.

While there may exist a legal basis for liability claims, enforcement of the liability claims can prove difficult. Anonymity of parties may render enforcement potentially difficult but this does not mean that the actions of individuals who together operate the distributed ledger are not legally relevant.

When establishing the maturity levels for this sub-risk area, we look at how well a business mitigates risks relating to legal liability. The sub-risk area closely relates to how a business handles regulatory compliance. The main difference is that the types of regulations are known while the current ways of establishing liability are often unknown. Therefore, with regulation you can simply be compliant but liability is mostly about the best way to reduce the impact of the risk. This is reflected in the maturity levels of this risk area.

Level 1. No formal evaluation of possible liability risks performed. Evaluations that are performed are inconsistently applied, informal and incomplete.

Level 2. Evaluation of liability performed after development of the application. Liability evaluated based on agreements with ecosystem partners. Liability risks are partly mitigated through contractual agreements between participants. No further evaluation of tort or partnership liability risks.

Level 3. Liability risks are taken into account during development of the application. Evaluation during development based on legal knowledge of the developers. All legal risks are evaluated by a specialized legal department before deployment of the application.

Level 4. Liability risks are constantly monitored by legal department.

Level 5. Monitoring of legislation and case law by legal department is carried out to identify possible DLT liability risks.

7.2.5 Development

Within the development risk area, 4 underlying sub-risk areas have been defined. The overall definition of the development risk area is the following:

Risks arising during and around the development of the DLT application.

Integration with existing systems

When newly created DLT systems need to interact with legacy systems it creates new attack vectors to the organization's network. This sub-risk area looks at how these integrations with existing systems are set up in order to reduce risks such as an insecure or non-functional integration.

A number of challenges and risks exist when integrating a DLT application with existing systems. From a data perspective, transaction finality and current security infrastructure within a company are possible risks. If external data or events based on time or market conditions needs to interact with

the DLT, an oracle is required. Creating oracles from existing data sources can lead to potentially insecure centralized data environments and this should be done with care. Framework which can help to solve this issue by automating the creation of these Oracles is Microsoft's Project Bletchley (Grey, 2017).

Next to issues with data sources, interfaces should be able to handle the issues with transaction finality in DLT solutions. It may be possible that a transaction is not completed while the legacy system has sent the data and therefore thinks the transaction has been completed. Proper feedback should be provided in order to make sure that no data is lost in the interaction between the legacy system and the DLT application.

How the DLT application works with current security infrastructure of the company can create insecure connections between legacy systems and DLT systems. Running a DLT application within a VPN of a company may open up new attack vectors to the legacy systems it is connected to.

Level 1. The DLT application runs separately from all other applications. Manual input needed to transfer information from existing systems.

Level 2. DLT application and existing systems are integrated separately developed and evaluated interfaces. Interfaces with existing systems are evaluated for known security weaknesses. Assessment has been performed to test the functionality of the integration.

Level 3. Single secure interface or standard for interface exists for existing systems to interact with DLT application.

Level 4. Interface with existing systems are being continuously monitored for errors and security incident detection features exist.

Level 5. Continuous monitoring for improvements to the interfaces and reducing complexity of interfaces where possible. Adaptive integration infrastructure that can handle changes when DLT standards evolve.

Code quality

Like in all software development, the quality of the code created is of importance. Within the DLT area this is especially the case with some of the code developed being difficult to alter. Once some executable code like smart contracts are deployed on the chain they cannot be changed in case there is an error in the code. Furthermore, deploying changes to other aspects of code may be more difficult because the code is often used by multiple parties which have to agree on the changes.

In order to reduce the need to change code after deployment application developers should strive for a high code quality. With DLT being a relatively new area there are few experienced software engineers. Less experienced engineers may be more prone to making coding errors which lead to a lower quality of the code.

Many of the currently developed DLT applications are being created as proof of concepts or MVPs, the code that is being written is often not of high quality and changes to the protocol may cause code to quickly become obsolete. The fast changing codebase of DLT platforms and applications utilizing them should be constantly updated and be kept up to date. With the quickly developing code of many DLT platforms and fast iterations, poor documentation of code can become an issue. This is especially relevant to developers which are not yet very well versed in blockchain development.

The area of code quality is well established and has been a focus in code creation since the establishment of maturity models. This means that there are already a number of maturity models

available which relate to code quality. Elements from these models together with the identified risks have been used to create the following maturity levels:

Level 1. Knowledge on code is silo-ed, includes many home-grown solutions and unmodifiable legacy code. Code is buggy but functions if you know how to avoid the buggy areas. Lack of skilled engineers available to create application.

Level 2. Code works and matches the requirements of the application. Code includes duplicate solutions to same problems. Code is difficult to understand by another software engineer.

Level 3. Code is well documented and modern design patterns are used to create code. Code is readable by another software engineer. Skilled software engineers available to create the application.

Level 4. Code is modular and reusable in other DLT applications. Software engineers with experience in DLT development available.

Level 5. Quality of code can be quantitatively measured and the development is being continuously improved.

Code verification

This sub-risk area focuses on the verifiability of code created for the DLT application and debugging of the code and transactions in the DLT. Some DLT protocols, like Ethereum, offer new domain specific languages which may be difficult to test and verify for correctness.

Due to the nature of the DLT, smart contracts cannot be tested to produce the same outcome each time it is being run. It depends on the state of the network which may change between the different execution times of the smart contract. Furthermore, once smart contracts are published they cannot be changed making coding errors in smart contracts permanent. This calls for heavy testing and debugging of code before it should be released.

Level 1. Code is proprietary and has not been formally proven.

Level 2. Code is audited based on functional testing.

Level 3. Code is audited based on non-functional testing.

Level 4. Test-driven development with continuous testing throughout development

Level 5. Continuous improvement of code verification with additional programs to further test the code when released.

Part III

Evaluation

Chapter 8

Model Verification and Validation

In order to verify and validate the maturity level descriptions and create a final model, a number of experts have been consulted to give their feedback on the preliminary model. Based on the feedback, the level descriptions of the different risk areas have been adapted. The model is adapted to be used for assessment of applications by creating assessment questions which are derived from the level descriptions and visualizing them through a dashboard. This dashboard was presented to a DLT expert involved in multiple projects involving DLT application to validate the design.

8.1 Verification through Survey

In order to validate the created maturity levels as presented in the previous chapter, a survey was send out with questions about the created maturity level descriptions. The survey included all of the participants of the Delphi study and the interviewees contacted related to the evaluated case studies. The total participants to which the survey was send out was 22. The survey was open for one week in which 11 participants of the survey responded. From a number of the participants we got the response that they did not have time to complete the survey while from others we did not get any response.

The survey consisted of all the maturity level descriptions presented in the previous chapter including the overall maturity level descriptions. This lead to a total of 15 questions each with the possibility to rate the descriptions on a scale from 1 to 5, 1 being completely disagree to 5 being completely agree. Furthermore each participant was asked to motivate their answers and if they disagree to give improvement recommendations.

8.1.1 Results and Improvements

Table 8.1 presents the results of the survey. A number of risk areas scored below a 4.0 with some of these areas showing a high spread among the answers. Each of the areas has been further investigated and a better look is given to the areas which showed a lower degree of agreement. The rest of this section will highlight the comments given to the level descriptions and states where we have made adaptions to the descriptions. All the changes to the model are presented in the last section of this chapter.

Table 8.1: Results of the survey

Category	Average	Spread
Overall Maturity Levels	4,36	0,48
DLT Platform Choice	3,82	0,83
DLT Ecosystem Partners	4,27	0,20
DLT Application Performance	4,18	0,57
Data Management	3,73	1,05
Change Management	4,00	0,60
Endpoint Security	3,64	0,77
DLT Protocol Attacks	4,45	0,50
Identity Management	4,18	0,72
Transactional Security	4,09	0,79
Regulatory Compliance	4,36	0,64
Legal Liability	4,09	0,29
Integration with Existing Systems	4,09	0,67
Code Quality	4,27	0,45
Code Verification	3,64	0,48

8.1.2 Overall Maturity Levels

The overall maturity levels will stay the same. Each participant agreed with the levels and there were no comments to change the level descriptions.

8.1.3 DLT Platform Choice

DLT platform choice is one of the areas which had a low degree of agreement, only 3,82, and a high spread of the answers, 0,83. Two participants neither agreed nor disagreed and one disagreed with the descriptions. The participant that disagreed stated that a number of classical enterprise platform selection criteria are missing. We will not be including the classical enterprise platform selection criteria in the level descriptions. While these are relevant for the overall selection process, they are not limited to a DLT platform. We have made the decision to limit our scope with this model to only include criteria for DLT related risks.

The participants that neither agreed nor disagreed stated that the order of the levels might be dependent on the use case and that the highest level does not seem to fit with the rest of the levels. Based on this feedback we have adapted the descriptions to level 4 and 5 to create a more clear linear order to the levels.

8.1.4 DLT Ecosystem Partners

Overall, participants agreed with the level descriptions of the DLT Ecosystem Partners risk area with an average score of 4,27 and a spread of only 0,20. One participant neither agreed nor disagreed stating he would change descriptions of level 3 and 4. These levels relate to the agreements between participants to keep using the system and the process of what happens when a participant drops out. The comments do not change the meaning of the levels but provide a clearer language which has lead us to redefine levels 3 to 5.

8.1.5 DLT Application Performance

Participants of the survey scored the level descriptions of DLT Application performance with an average of 4,18 and a spread of 0,57. There were a number of comments to change level 5 and to make the distinctions between level 3 and 4 more clear. The comments relating to level 5 stated that it seemed like a combination of level 3 and 4 and did not provide additional distinctions. Based on these comments we have revised level 3 to 5 with more clear language.

Furthermore, two comments were given about the factors to measure application performance stated in the description of the risk area. It stated that transaction finality is not covered by the four criteria we have mentioned. While this was not part of the factors which we extracted form the research by Adulla et al. (2018), based on the comments we recognize the benefit of including this measurement.

Depending on the type of DLT there are different types of transaction finality (Gauba, 2018). We will not go into detail within this research about the different types of transaction finality but instead we define it in general as the following: “the transaction finality is the time it takes before it is very unlikely that a transaction is revoked at a later time.” Depending on the type of consensus mechanism it is possible to completely guarantee the transaction finality or give a probabilistic transaction finality.

8.1.6 Data Management

The Data Management risk area was quite a controversial area with an average score of 3,73 with a spread of 1,05. Only five people agreed with the level descriptions and the others either disagreed or neither agreed or disagreed. The comments motivating these responses mostly relate to the blocking of data to the network. They state that identifying what is illegal and blocking this on a network level would be difficult if not impossible.

This is a difficult topic where no solution has been identified yet by any of the participants or experts we have talked to. One method of blocking data is using a front-end block, but it is still possible to circumvent the front-end and put data into the ledger. Realizing a network-wide block may not be possible and lead to other issues. Other participants state that you do not want to block data from the network and should allow all data on the network. When all data is allowed on the network there should be measures in place to remove or restrict access to data in the network.

Furthermore, decentralizing the identification of illegal data may prove a difficult task. What is deemed illegal data for one participant may not form the same issues with other participants in another jurisdiction. In order to realize a truly decentralized network, the identification of the data should also be as decentralized as possible. When you do not do this you allow a small subset of participants to have the power to block or remove data for all the participants in the network.

One other participant who disagreed with the levels stated that the part about auditability of data did not make sense to him, stating the benefit of a blockchain is that this should not be needed. While we believe that a benefit of the blockchain is the immutability of data, it does not provide guarantees for the accuracy of data. The accuracy of data should in our eyes still be auditable by a third party to ensure the data that is put onto the ledger is correct.

Another participant stated that the possibility to remove data should be already included in lower levels since this is a key component of GDPR compliance. Even though the removal of data is a requirement of GDPR, the exact interpretation of the law by European courts is not clear yet. It may be possible that a system is GDPR compliant when access to data can be sufficiently restricted instead of completely removed. We believe that reaching compliance would be better by completely restricting the use of private data on the DLT.

The notion of 'illegal data' is also not clear to all the of the participants. With this term we mean to identify data which may be in conflict with legislation or contractual agreements between participants. We have changed the descriptions to a number of the levels to make them more distinctive but have decided to not majorly change how the levels are structured. This is a topic which should be further investigated when there is more clarity on the interpretation of the GDPR.

8.1.7 Change Management

In the Change Management risk area most participants of the survey agreed with the level descriptions, the area reached an average score 4,0 and a spread of 0,6. Two participants neither agreed nor disagreed, one of the major concerns were with the fact that a more decentralized governance structure equals a higher maturity level. The participant argues that depending on the use case it is also possible that a centralized governance structure with clearly defined processes would be better than a decentralized governance structure. While we agree that it is use case specific, we believe that overall a more decentralized system will be better for the large majority of DLT applications. Therefor we have decided not to change the level descriptions for this risk area.

8.1.8 Endpoint Security

Together with the Code Verification area, the Endpoint security area rated the lowest out of all the areas with an average of 3,64 and a spread of 0,77. Even though no one disagreed with the descriptions, the majority of the participants neither agreed nor disagreed, stating the difficulty of creating maturity levels for this area.

The progression in the levels is not very clear to everyone. Some state that while the levels each describe different methods of securing endpoints, one may not be better than the other. We believe this is a good progression of the levels also due to the maturity model research performed by Carielli et al. (2018). Many of the descriptions of the levels are based on this research. We have clarified some of the descriptions of the levels to better reflect our intention behind the levels.

Another comment states that the levels are only focused on restricting access to the DLT, this may not be the only and best way to secure endpoints. Other methods, such as consensus mechanisms which allow for malicious nodes, should also be taken into account. We agree that it is not the only method of securing the endpoints but believe that other methods of securing should be handled when selecting a DLT platform and therefor falls under the DLT platform choice risk area. Therefor, we have not included this within this risk area.

8.1.9 DLT protocol attacks

The area of DLT protocol attacks has one of the highest agreement levels, average of 4,4 and spread of 0,5, and comments also do not mention any improvements needed to the level description. Therefor the level descriptions are not further adapted.

8.1.10 Identity Management

The level descriptions relating to the Identity Management risk area are generally agreed upon with an average of 4,18 and a spread of 0,72. Two participants neither agreed nor agreed stating that a difference should be made between what a single participant should do for identity management and what should be done on a network scale. We agree that there is a distinction between the two, but we have decided to only focus on the application layer and less so on the network layer. The

difference between levels 4 and 5 was not clear to some of the participants. We have adapted the level descriptions with more clear language to resolve this.

8.1.11 Transactional Security

Most participants of the survey agreed with the level descriptions of the Transactional Security risk area with an average of 4,09 and a spread of 0,79. Two participants neither agreed nor disagreed stating that they don't get the description to not add any sensitive data to the ledger. This also relates to another comment stating that the levels could be different if you decide that the information should be added either way.

The choice for this level has been made consciously since if an organization is not able to secure information in the transaction that they want to have secure we believe they should not put it in at all. We have decided to keep the level descriptions for this risk area the same.

8.1.12 Regulatory Compliance

All participants agreed with the level descriptions given for the Regulatory Compliance risk area which averaged a 4,36 with a spread of 0,46. We have decided to keep the level descriptions for this risk area the same.

8.1.13 Legal Liability

For this risk area all the participants agreed with the level descriptions but do offer some suggestions for improvement. Two participants commented that the level descriptions only describe identifying and monitoring the risks but do not include acting on them. Based on the comments we adapted the level descriptions to reflect the suggested changes.

8.1.14 Integration with Existing Applications

For this risk area most participants agreed with the level descriptions with an average of 4,1 and a spread of 0,7, but the comments showed that there is room for improvement. One of the comments stated that the applications which should be integrated needs to be specified since the levels may be different because of it. We believe the levels are application dependent but further specifying the applications will limit the model too much. In order to increase clarity we have chosen to consistently use the wording application instead of system.

Other comments stated the difficulty to comment on the accuracy of the levels since it can differ a lot from case to case. We have adapted levels slightly to improve clarity but we have not changed levels drastically.

8.1.15 Code Quality

All participants of the survey agreed with the level descriptions as proposed with an average of 4,3 and a spread of 0,4, but again the comments do offer some points of improvement. These points all relate to improving the wording in the descriptions and do not change the meaning of the descriptions. We have adapted the level descriptions to include the suggested improvements.

8.1.16 Code Verification

The Code Verification risk area scored relatively low, only an average of 3,6 with a spread of 0,5, but no participant disagreed with the descriptions. The comments give a little bit of an explanation as to why this is the case but they are not conclusive. Comments state that level descriptions could be adapted to include more factors such as external audits and collaborative development of smart contract code. Another comment states that a factor mentioned in an earlier level, functional testing, does not come back in a later level. How the maturity model is set up is to build upon the previous level. Therefor to get to level 3 one should also be compliant with the previous levels. We have made this more clear in the descriptions.

8.2 Extending the Model

In order to evaluate how the maturity model fits to practice, a number of assessment questions have been derived from the level descriptions of each risk area. These assessment questions allow for the model to be easily applied to use cases through self-assessment or assisted through a third party.

8.2.1 Assessment Questions

The assessment questions are developed based on the descriptions of the different maturity levels. Each element described in the maturity level description is extracted and placed in individual assessment criteria. During an assessment, the assessor will note if an application fulfilled the statement or not. While in general each level builds upon the previous level, some elements of the descriptions should not be reproduced in higher levels. When, for example, an application is evaluated on their Ecosystem partners, level 1 dictates that the network is run internally while in level 2 and higher the network should run with partners as well. In order to support the nuances in the maturity level descriptions, the assessment questions have been assigned a criteria if they are required for the higher levels or not. Table 8.2 presents and example of the statements for one of the risk areas, a complete list of statements can be found in appendix D. The '0' in the required column means it is not necessary to fulfill this statement if a higher level is fulfilled.

Table 8.2: Example of statements for DLT Platform Choice risk area

Level	Statement	Required
1	The platform has been chosen based on the experience of the developers.	0
1	The platform has been chosen based on what is available.	0
2	A requirement analysis for the use case has been performed to analyze what type of platform is needed.	1
3	The criteria for fit of a DLT platform to a use case have been standardized.	1
4	The platform needs for the use case are periodically examined.	1
4	Processes in place to optimize existing platform or switch platform if needed	0
5	The platform is continuously evaluated through pre-defined criteria	1
5	The platform is periodically compared to other platforms to evaluate the best fit	0

8.2.2 Visualizing the Model

In order increase the comprehensibility of the outcome of an assessment and to easily identify areas for improvement, a dashboard has been developed. Using the answers to the assessment statements within an assessment excel sheet as input, the dashboard automatically visualizes the levels reached for each risk area. The dashboard is presented to a DLT expert involved in multiple projects relating to DLT applications for validation.

Back-end Design

The dashboard has been designed using the business intelligence and analytics software of Tableau (Tableau Software, 2018). This software allows for the creation of dashboards from multiple data sources. Within this software the reached levels for each sub-risk area are calculated and visualized. Through an interactive dashboard the individual levels and level descriptions can be identified along with which statements relate to the levels.

There are two data sources for this visualization. One of the data sources is constant and houses the information related to the created maturity model. For this data, a MySQL 8.0 database is used with the schema design presented in figure 8.1. The SQL used to create and populate the database can be found in appendix E.

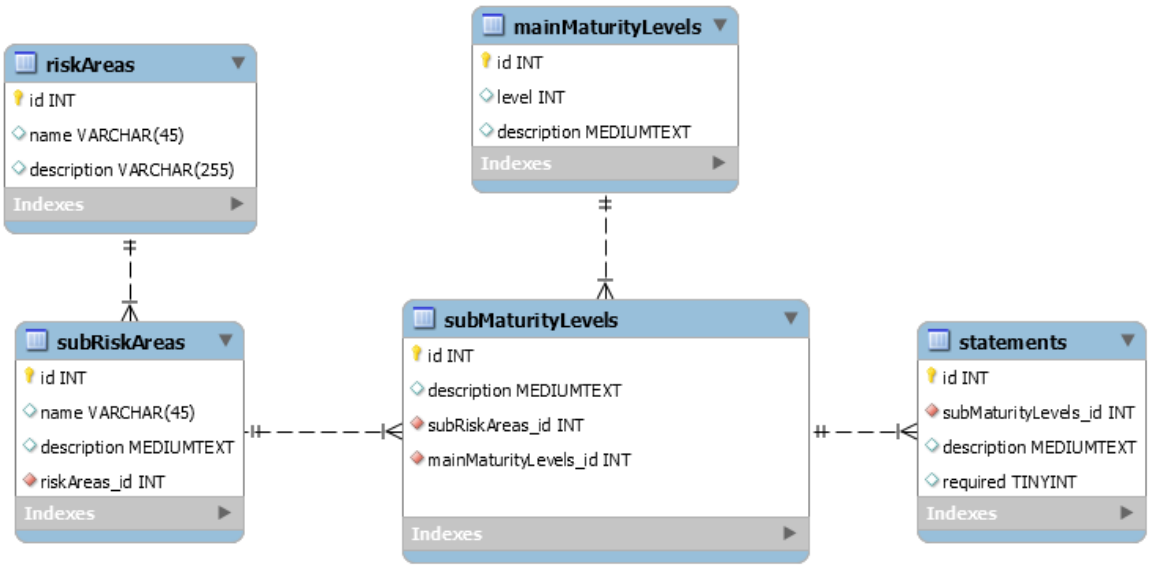

Figure 8.1: Database Schema

The second data source is an Excel sheet with the raw results of a maturity assessment. This sheet includes all the statements found in appendix D including an extra field which states if the statement is fulfilled for the application. This data is combined with the data from the database within Tableau using the statement ID as a union field.

Front-end Design

The design of the dashboard is focused on creating a quick overview of the outcome of a maturity assessment while still providing enough information to identify points for improvement. It is a two layered design with a main page shown in figure 8.2 which shows the overall maturity level of the application on the left and the individual maturity levels per risk area on the right. When hovering

over the bars representing the levels, the text description of the level is presented. When a bar is faded, the level has not been reached.

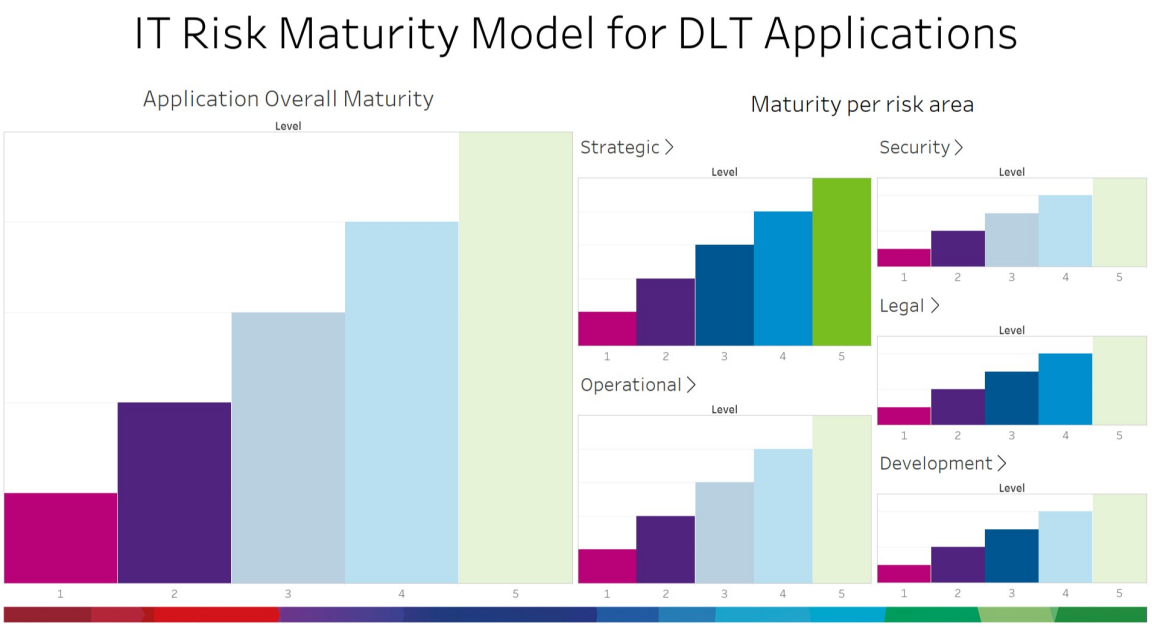

Figure 8.2: Main screen of Maturity Dashboard

The second layer of the dashboard zooms in on the individual risk areas. These screens can be reached by clicking on the arrows or names of the risk areas within the main screen. An example screen of the strategic risk area is shown in figure 8.3. The screen includes the maturity levels for the different sub-risk areas which fall under the strategic risk area. Additional information about the level descriptions of each level can be obtained by hovering over the individual levels.

On the bottom of the screen an additional bar shows how each statement related to the sub risk area is answered. By hovering over the bar information can be obtained about what statement needs to be fulfilled before the next level is reached.

8.3 Evaluating the assessment questions and Dashboard

Earlier in the research (chapter 6) a number of case studies have been performed on different DLT applications. One of these case studies has been further evaluated in order to verify the created assessment questions and dashboard.

The assessment questions have been been completed by a party closely related to the project. The answers to the assessment questions have been analyzed though the created dashboard to evaluate the current risk maturity level of the application. Through the analysis of the dashboard we found that the results of the maturity assessment does not fully reflect the estimates of the researcher. There are a number of risk areas where the reached level was higher than expected and a number of areas where it's lower instead. The dashboard allowed us to further examine why this is the case.

We found that a number of statements that have been answered as 'True' does not accurately reflect the state of the project. This may be in part due to bias by the party involved in the project. The assessment is filled in as a self-assessment, this allows for the party filling in the assessment to steer the results in a certain direction. In order to reduce the possibility of this bias, the assessment

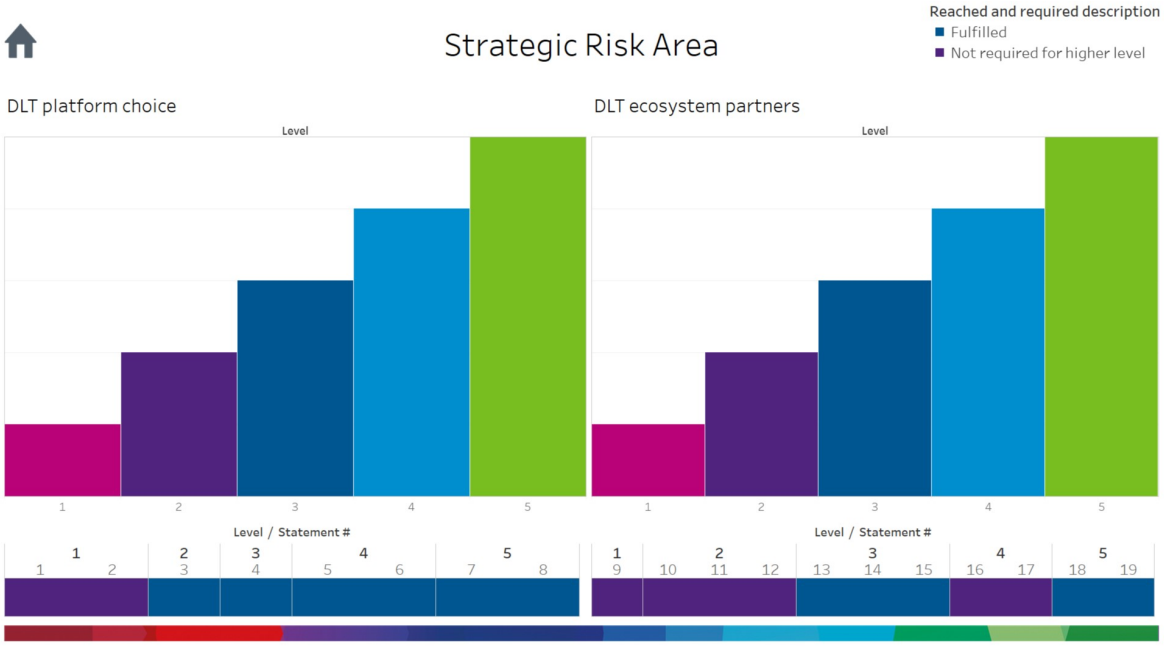

Figure 8.3: Detailed screen of Maturity Dashboard

can be performed by a third party with a unbiased view on the project. Furthermore, more members of the project can be asked to perform an assessment in order to balance skewed results.

As explained in section 8.2.1, some of the assessment statements are required in order to reach a higher level and some are not. When looking closer at some of the risk areas, we found that some areas scored lower because some questions that have been marked as required in a lower level have not been reached. When looking closer at the assessment questions, some questions marked as required may not necessarily have to be required for a higher level. This was especially apparent in the 'DLT performance' risk area where instead of a level 5, only a level 2 was reached because of one required statement. This statement was relating to increasing performance by adding additional resources. However, the application is not able to do this since it runs on a semi-public network. Therefore, for this application it may not be an accurate required statement.

The dashboard is an easy way to identify specific problem areas. However, accurately gathering assessment results can still be improved. The largest improvements would be had by adapting some of the assessment questions and reevaluating which ones are required for a higher level and which are not. Furthermore, the assessment can be improved by including multiple parties in the assessment or by adapting to a third-party assisted assessment.

Chapter 9

Discussion

In this chapter, the research is reflected upon and the research questions proposed in the beginning of the research are answered. We discuss the relevance of the research and look at limitations and future work.

9.1 Conclusions

This research has presented a multi-method approach to develop a maturity model for DLT applications. Through multiple studies, combining literature and practice, the risks of DLT applications are identified and categorized. The created maturity model will assist businesses in identifying risks and identify specific risk areas where they can improve the DLT application.

Five sub research questions were created to give guidance in developing the maturity model. These research questions will be answered and reflected upon in this section.

> **Sub question 1:** *What is Distributed Ledger Technology in connection with the Internet of Things?*

Chapter 2 presents background information on DLT and IoT. These topics are brought together in section 2.2.2 which explains that DLT can act as an enabler for IoT by providing a robust mechanism to support decentralized networks. This decentralized network reduces single points of failure and the cryptographic algorithms used within DLT protect data. Furthermore, it reduces the costs of maintaining a single centralized cloud to support the IoT devices.

> **Sub question 2:** *What maturity models are currently available to evaluate IT risk maturity of software applications?*
>
> **Sub question 3:** *What is the state of the art of maturity models with respect to risks of DLT applications in the IoT domain?*

In order to answer these questions, a literature study has been carried out (chapter 3) which evaluates and compares current available maturity models. We identified a number of maturity models, including one from van der Voort and Spenkelink (2018) which was specifically aimed at risks of DLT applications. After an evaluation of the model by van der Voort and Spenkelink (2018) a number of limitations to this model were found. The model focuses on the financial sector using private DLT and it does not look at risks of public DLT. The model and the complete research behind the model are also not freely available to the public.

Other identified models in the literature study looked at the risks of software application on an abstraction level that is too high to be valuable in the evaluation of DLT applications. Many businesses do not know all the risks involved in DLT applications. In our view, the identified models do not give enough guidance for risks specific to DLT and IoT. These include risks related to the immutability of data on the ledger, open and distributed governance systems, and working together with untrusted 'partners.' IoT specific risks relate mostly to the security of these devices. Based on the models that were evaluated, a research gap was identified for a model which is freely available, is well founded in scientific literature while still applicable to practice and is applicable to DLT and IoT applications.

Sub question 4: *What are the IT risks and corresponding risk domains for DLT applications in general and specific to IoT?*

The first step in designing the model is to identify what should be included in the model. The elements on which the model is built are the IT risks of DLT applications and respective risk domains of these risks. In order to identify the risks, three studies were performed. The first study identifies IT risks as described in literature through a systematic literature review. The second study includes a number of industry experts in a Delphi study to identify risks according to practice. The third study applies the identified risks to five use cases to evaluate how they apply to practice.

During a systematic literature study in chapter 4 we identified 29 risks divided over five risk areas. In our initial search we identified more risks but we found that many of them were duplicate or closely related to each other. The abstraction levels of the initial list of risks varied greatly. Some studies, like (Fernandez-Carames & Fraga-Lamas, 2018), provide a deep dive into specific technology risks while others, like Deloitte (2017), provide high level risk areas. We decided to create a number of risk areas which reflect high level risks and provide some more specific risks under these risk areas. Each of the identified risks and the corresponding literature can be found in appendix B.1 and B.2.

The identified risks from literature are presented to a panel of experts through a Delphi study in chapter 5. The experts ranged from different industry sectors, functions, countries and expertise in both IoT and DLT in order to achieve a high diversity in the expert panel. The responses provided a wide variety in risks but again presented the problem with the abstraction level of risks. Some of the risks that were mentioned, such as 'Hype' around DLT, were very high level while others, like '51% attack', are much more specific. There were no large disagreements when further narrowing down the risks and risk areas. This led to the identification of a total of 48 risks divided over 5 redefined risk areas and 18 newly defined sub-risk areas. Throughout the different rounds of the Delphi study we found that the IoT specific risks earlier defined in the literature study had been brought under different risk areas. A common risk of IoT devices is the device being breached, this is also a risk in other devices and is therefore brought under the 'endpoint security' risk area in order to generalize the model. The sub-risk areas provide more insights in the topics covered by the different high level risk areas and provide a method to further categorize risks.

In order to assess how the identified risks relate to risks of existing use cases, five case studies were performed in chapter 6. These case studies evaluated how the previously identified risks are reflected in the use cases. We have concluded that many of the risks are relevant for the different use cases, but there are a number of risk areas that do not apply to all DLT applications. Not all applications require high transaction speeds or make use of IoT, which make elements from risk areas like DLT Performance and DLT Platform choice irrelevant. Furthermore, we found that a model may be less relevant to analyze developing proof of concept applications. As these applications do not aim to create a production ready system, some design choices are made that create more risks but these may not be relevant in this stage of development.

Sub question 5: *How can the maturity levels be defined for each risk domain?*

During the use case studies it was found that the model will not be fitting for all DLT applications in general. For the model to be applied to a use case, a number of criteria were identified that a use case should adhere to before it can be appropriately measured by the model. These criteria are that it should strive for a high transaction speed, it should include IoT devices or intend to use IoT devices and the application should be used in a business to business or business to consumer relationship. These criteria make sure that the model accurately measures similar use cases.

With the IT risks and risk areas defined and evaluated through a number of use cases, their corresponding maturity levels are defined in chapter 7. In order to achieve a common measure for each risk area we defined high level maturity descriptions which the underlying risk area level descriptions are based on. The high level descriptions were derived from the CMMI level descriptions and adapted to fit this research. The levels for each of the risk areas were created based on the identified risks and existing maturity models.

> **Sub question 6:** *How can the IT risk maturity of a DLT application be assessed using the created model?*

In order to apply the DLT risk maturity model to a DLT application, a number of assessment questions have been created and presented in section 8.2.1. These assessment questions are extracted from the level descriptions for each risk area. The results of the assessment can be visualized in a dashboard presented in section 8.2.2. This dashboard allows an assessor to identify areas for improvement of the assessed application. While the dashboard functions well in displaying the results of the assessment, by applying the model to a previously studied use case we found the assessment questions may not accurately reflect the actual maturity level of an application.

> **Main Research Question:** *What constitutes a usable maturity model for IT risk assessment of distributed ledger applications in connection with the Internet of Things?*

All of the sub questions culminate to answering the main research question. We have created a maturity model which can be used for IT risk assessment of distributed ledger applications using IoT devices. There are three requirements for a DLT application in order to be accurately measured using the created mode. IoT devices should be used currently or in the near future within the DLT application, DLT application should be benefited by higher transaction speeds and lastly the application should created by a business and used for business to business or business to consumer interactions.

The model constitutes of 5 main risk areas with 14 underlying sub-risk areas. For each sub-risk area, level descriptions were defined to establish how well an application mitigates the identified risks for that sub-risk area. The maturity model can be applied to a DLT application by completing a number of assessment questions which yield a specific maturity level for each of the sub-risk areas. The outcome of the assessment can be visualized for easy identification of improvement areas.

9.2 Limitations

Throughout the research the aim has been to create a model which is well founded in scientific literature while also being applicable to businesses. From the beginning of the research, a clear path for maturity model development was developed with the research from Mettler (2011). Based on the development cycle presented in their research, a research methodology was created. This proved to be a helpful way to keep on track during the research, and identify all the elements needed to create a well-founded maturity model.

The research by Mettler (2011) also includes an application cycle next to the development cycle. While this cycle was outside of the scope of our research, Mettler argues that both the cycles should be more integrated. During the research we have included companies in the design process but have not further investigated how the model can be integrated into their development processes. Further improvements to the research design are presented in section 9.5.

During the design phase of the research we planned to use a Delphi study for the maturity model design process. The method used to design the Delphi model was based on the design method used by Rosemann and Bruin (2005). During the Delphi studies we found that the collected risks could not be properly transformed into maturity levels as described by the method of (Rosemann & Bruin, 2005). More information was needed about which applications the model is applicable to. We found that generalizing to all DLT applications would cause difficulties when discussing maturity levels. Without this knowledge there would be disagreements within the Delphi study which would not have been solved easily. In order to gather additional information, a number of case studies were completed before presenting the created maturity level descriptions for feedback to the participants of the Delphi study.

Due to the Delphi study not following it's intended design, we were unable to reach a complete consensus on the elements of the model. In the latest survey of the complete model there were some participants which disagreed with elements from the model. In the latest round of a Delphi study one should strive for the lowest amount of disagreements on the contents. We believe that with additional Delphi rounds the model could be more refined, this is presented in section 9.5.

The assessment questions are literal adaptions of the maturity level descriptions. During the application of these assessment questions we found that many of them are unclear when presented to an individual for self-assessment. While this can be solved using an assisted assessment, the questions can be reformatted to allow for individuals to complete an assessment without a researcher present.

The intention during the beginning of the research was to create a model with a focus on the combination of IoT and DLT while still generalizable to other non-IoT DLT applications. After the collection of risks through the literature and Delphi study, it was found that generalizing for all DLT applications was not possible. A number of level descriptions within risk areas are built up in such a way to only be applicable to applications which use IoT devices. Therefore, one of the criteria of the model is that IoT should be included in the application in order for the model to be applicable. Future work may include generalizing the model and removing the criteria defined in section 8.2.1.

9.3 Practical relevance of the research

When conducting the research we found that there are not many applications which use DLT that have made it into production. Many of the applications do not make it past the proof of concept phase due to varying reasons. This may be because the costs do not outweigh the benefits or because the technology does not provide the expected results.

The created maturity model can be used by organizations to easily identify shortcomings in DLT applications and guide the development towards more mature applications which may make it into the next stage of development and into production. We believe that the model will be of value during the development of an application once an essential question has been answered, does DLT provide additional benefits that cannot be achieved with traditional systems? In many cases the use of DLT does not provide additional benefits or the benefits do not outweigh the shortcomings of the technology.

This research was able to combine knowledge from the scientific community as well as practice.

Multiple companies from different fields were included in the research, in the results of the different surveys we noticed that there were differences between the different companies in how they answered the questions. Combining the knowledge from the different companies led to new insights valuable for all the included organizations and helped to reduce the silo-ed knowledge.

The created maturity model can be applied by any of the organizations included in the Delphi study, the assessment questions and dashboard files have been distributed to them. They are also able to change the dashboard based on the code included in this thesis. The largest contributed for these companies is for their research department. Since many companies are still investigating where and how to apply DLT, this research can be used to extend their current research efforts and to build upon this research.

Bosch is working on DLT in two ways, one is internal consulting for DLT applications and the other is researching new initiatives. In both these practices the model can be of use. Within internal consulting it can be used to evaluate existing DLT applications and decide if it's worthwhile to implement within Bosch. It can also be used within the development of it's own solutions as a guide to develop more mature DLT applications.

Within the research department of Bosch it offers multiple elements that can be of use to the research. The classified lists of risks offers a perspective of DLT application risks as identified by a number of external companies. This is valuable information which serves as a basis to decide what to focus research on. The completed maturity model offers a perspective on how to mitigate the identified risks within certain applications. While it is not generalized to all DLT applications it may be developed further using suggestions presented in section 9.5.

9.4 Scientific relevance of the research

This research provides valuable insights for academics on a number of different fronts. The main contributions to the scientific community are the identification of DLT application IT risks and a maturity model to assess these risks. Besides these contributions there are elements within the research, such as a combined assessment model for maturity models, which can be applied further as well.

During the evaluation of existing maturity models we did not find a model that can be used to test both the quality of a model and its applicability to the use case. We combined the model from Pöppelbuß et al. (2011) with applicability criteria from Mettler (2011). We believe that only looking into the applicability of a model is not enough to choose one. The quality of the model should also be taken into account, which is especially exemplified by the model of Wang et al. (2016). This model is aimed at DLT but does not provide enough quality to be applied to DLT applications.

There have been a number of papers which have collected risks and challenges of DLT (Conoscenti et al., 2016; Karafiloski & Mishev, 2017; Koteska, Karafiloski, & Mishev, 2017; Yli-Huumo, Ko, Choi, Park, & Smolander, 2016). One extensive example of this is the paper by Fernandez-Carames and Fraga-Lamas (2018), which focuses specifically on IoT and DLT issues. While this paper identifies many of the same issues, we found that a number of risks that are important to businesses are not included in this model. One of these risks is the risk of ecosystem partners, especially concerning how to attract them and keep them on board. The article also misses any legal risks associated with the application that are specific to DLT. Most of the scientific literature that was found focuses on technology risks of DLT, the business aspects are often not represented in the same way. The literature that was found during our research often presents an ideal picture where DLT would solve a number of issues where other participants are not trusted, but within practice this did not seem to be the case. Many of the issues of the investigated use cases are to business related issues such as a poorly functioning governance system. Therefore, we believe that our assessment can be seen as

a valuable addition to the current landscape of literature.

This research especially brings its value through combining knowledge found in literature with knowledge from practice. We did not find any examples of literature where multiple companies were included in the identification of DLT risks. This was combined with a multi-method approach, which allowed for a well-founded maturity model. Certain risk areas within the model provide a base for further research. We found that the areas of data management, endpoint security and change management are still disputed. This is further explained in section 9.5.

The main contribution of this research to academics is the model, which is openly available to anyone. The research will not be published by a journal but it is freely available from the university website and is distributed among the companies and universities included in this research. We found that previous models are often not openly available or there are only small elements of the research behind it available. With this model we welcome other researchers from organizations or academics to extend upon our research and provide a basis for future research.

9.5 Future work

During the work on this thesis we identified a number of areas on which research could be extended. We believe that the area of DLT research is still young, which is supported by the results of our literature study. During this literature study, a large number of studies was gathered but a complete systematic literature research as defined by, for example, the PRISMA method (Moher et al., 2009) was not performed. The information needed for this research, risks of DLT applications, was extracted but a qualitative synthesis of the results was not performed. A complete literature review including the last steps of PRISMA can benefit other researchers by providing a clear state of the art of the fast changing field of DLT research. This can be combined with our findings of risks according to experts from practice to form a more complete overview of risks.

From the literature we found that the link between practice and academics is often times hard to make. While technological solutions are frequently stated as solving many of the issues with DLT, we have found that in practice the areas which could be most improved on are in governance and collaboration. This is also evident by the disagreement of some experts with our change management risk area. One of the risks that came up with DLT experts from organizations during the Delphi study was the hype around DLT. This hype brings along issues with inflated expectations and mismatched solutions to problems of the technology. This is not only the case with DLT but is also discernible with other hyped topics. The hype brings along more attention to the topic but businesses might not be involved in the technology right away. A technology might not be commercially viable for businesses until later stages of maturity. Since businesses join later, the gap between business and academics is the largest in these early phases of a new technology. While academics cannot force businesses to adopt the new technology, they can help to find commercially viable solutions which can be adapted by businesses. Including businesses in research, for example within our research, exposes issues which might otherwise not have been identified in such an early stage. Working together to solve these issues may help to reduce the gap between academics and business. Future research can examine how new governance models can be created and applied within a group of organizations or a DLT network as a whole.

The developed maturity model can be applied to a number of use cases which use IoT devices and operate with certain requirements. We found that while risks of many DLT applications are similar, reducing them can vary greatly per type of use case. Future research can focus on making the maturity model generalizable to more use cases. This can be established by a more extensive investigation into the solutions to some of the risks or by making elements of the maturity model more

modular. When a more modular model is created it may be more difficult to compare results between applications but it may help to better identify improvement paths for the specific use cases.

Next to the development cycle used within our research, the research of Mettler (2011) proposes an application cycle shown in figure 9.1. These two cycles work together in order to create a maturity model which can be integrated within an organization. Our research touched upon applying the model within an organization, but did not follow the entire cycle as presented in the application cycle. We believe the current model already provides benefits when applied within an organizations, but elements of the model need to be developed further. Within Bosch, the model will be further developed and extended to evaluate use cases. In order to guide this development the combined cycle of Mettler (2011) can be used.

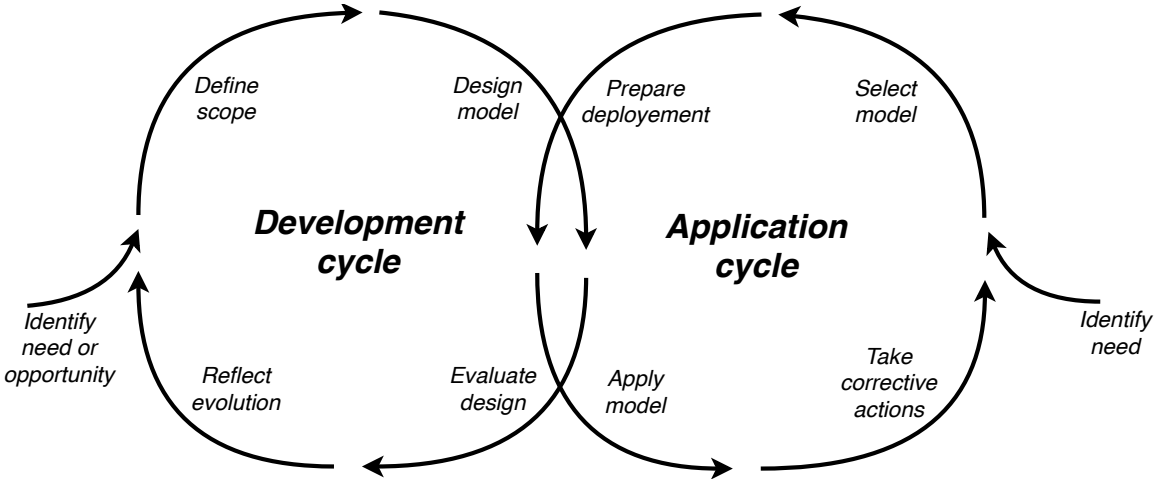

Figure 9.1: Maturity model development and application cycle (Mettler, 2011)

A number of risk areas created in our model provoked disagreements between the experts involved in the Delphi study, both during the course of the study and the creation of the maturity level descriptions. Further research should be done into these areas in order to reach a model that is more widely accepted. The risk areas which we believe should be researched further are the areas of 'Change Management', 'Data Management' and 'Endpoint Security.' The area of change management focuses creating a a well functioning governance system between participants of a DLT application. It can be argued that with this necessity of a well functioning governance, it might not even make sense to use DLT instead of a more mature technology. We believe a decentralized open governance system would be a good solution to this issue but other experts disagreed with this during our validation.

The area of 'Data Management' focuses both on how data should be added to a ledger and on the data itself. Since data on a DLT is often times irremovable, one should be careful with deciding which data should be added to the ledger and which data should not. Sensitive business information or private data should not be added to the ledger. One solution to this problem is to actively block this type of sensitive or private data from being uploaded to the ledger. We believe this would be a good option, but implementing this block throughout a DLT may not be possible. The issue which is currently limiting the blocking of data on a network wide level is the identification of the sensitive or private data. This type of data may differ for each user of the DLT application.

'Endpoint Security' is focused on the security of nodes connected to the DLT network. Within our model we focused on IoT devices as endpoint devices of the network. These nodes can be compromised which can lead to unforeseen issues within a DLT application. By blocking endpoints from the network due to certain security requirements or because of anomaly detection mechanisms,

the network can be protected. Not all participants of the Delphi study agreed with this approach since there are types of DLT protocols which allow for a number of the nodes to be malicious. Blocking nodes is only one way of addressing the issue of compromised nodes in the network; other methods of protecting the network should also be examined.

Bibliography

Adulla, M., Baset, S., Bharathan, V., Graham, G., Hochstetler, G., Kocsis, I., ... Wagner, M. (2018). *Hyperledger Blockchain Performance Metrics* (Tech. Rep.). Hyperledger. Retrieved 2018-10-22, from https://wiki.hyperledger.org/groups/pswg/performance-and-scale-wg

Alonso, J., Martínez de Soria, I., Orue-Echevarria, L., & Vergara, M. (2010). Enterprise Collaboration Maturity Model (ECMM): Preliminary Definition and Future Challenges. In *Enterprise interoperability iv* (pp. 429–438). London: Springer London. Retrieved 2018-08-01, from http://link.springer.com/10.1007/978-1-84996-257-5{_}40 doi: 10.1007/978-1-84996-257-5_40

Babaioff, M., Dobzinski, S., Oren, S., & Zohar, A. (2012). On bitcoin and red balloons. In *Proceedings of the 13th acm conference on electronic commerce - ec '12* (p. 56). New York, New York, USA: ACM Press. Retrieved 2018-4-26, from http://dl.acm.org/citation.cfm?doid=2229012.2229022 doi: 10.1145/2229012.2229022

Banafa, A. (2017). IoT and Blockchain Convergence: Benefits and Challenges. *IEEE Internet of Things*. Retrieved 2018-7-12, from https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management A Procedure Model and its Application. Retrieved 2018-02-04, from https://link.springer.com/content/pdf/10.1007{%}2Fs12599-009-0044-5.pdf doi: 10.1007/s12599-009-0044-5

Benbasat, I., Dexter, A. S., Drury, D. H., & Goldstein, R. C. (1984, may). A critque of the stage hypothesis: theory and empirical evidence. *Communications of the ACM*, *27*(5), 476–485. Retrieved 2018-04-12, from http://portal.acm.org/citation.cfm?doid=358189.358076 doi: 10.1145/358189.358076

Bloo, F. W. C. (2018). *Towards Updatable Smart Contracts* (Tech. Rep.). Retrieved 2018-10-24, from https://essay.utwente.nl/76769/1/Bloo{_}MA{_}EEMCS.pdf

Carcary, M. (2013). IT risk management: A capability maturity model perspective. *Electronic Journal of Information Systems Evaluation*, *16*(1), 3–13.

Carielli, S., Rudina, E., Soroush, H., & Zahevi, R. (2018). *IoT Security Maturity Model: Description and Intended Use* (Tech. Rep.). Industrial Internet Consortium. Retrieved 2018-08-05, from https://www.iiconsortium.org/pdf/SMM{_}Description{_}and{_}Intended{_}Use{_}2018-04-09.pdf

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, *4*, 2292–2303.

Churyumov, A. (2016). *Byteball: A Decentralized System for Storage and Transfer of Value* (Tech. Rep.). Retrieved 2018-03-27, from https://byteball.org/Byteball.pdf

CMMI Institute. (2014). *Data Management Maturity (DMM)* (Tech. Rep.). CMMI Institute. Retrieved 2018-08-01, from https://cmmiinstitute.com/store/data-management-maturity-(dmm)

CMMI Product Team. (2010). *CMMI for Development, Version 1.3* (Tech. Rep.). Pittsburgh,

PA: Software Engineering Institute, Carnegie Mellon University. Retrieved 2018-04-17, from http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9661

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. In *Computer systems and applications (aiccsa), 2016 ieee/acs 13th international conference of* (pp. 1–6). IEEE.

Curley, M. (2008). Introducing an IT Capability Maturity Framework. In (pp. 63–78). Springer, Berlin, Heidelberg. Retrieved 2018-04-17, from http://link.springer.com/10.1007/978-3-540-88710-2{_}6 doi: 10.1007/978-3-540-88710-2_6

Dalkey, N., & Helmer, O. (1963). An Experimental Application of the Delphi Method to the Use of Experts. *Management Science*, *9*(3), 458–467.

De Bruin, T., Freeze, R., Kulkarni, U., Rosemann, M., Freeze, R., & Carey, W. P. (2005). Understanding the Main Phases of Developing a Maturity Assessment Model. In *Acis 2005 proceedings.* Retrieved 2018-03-13, from http://aisel.aisnet.org/acis2005

De Haes, S., du Preez, G., Massa, R., Peeters, B., Reznik, S., & Steuperaert, D. (2009). *The Risk IT Practitioner Guide* (Tech. Rep.). ISACA. Retrieved 2018-07-18, from http://www.colmich.edu.mx/computo/files/MAAGTIC/RiskIT{_}PG{_}30June2010{_}Research.pdf

de Kruijff, J., & Weigand, H. (2017). Understanding the Blockchain Using Enterprise Ontology. In (pp. 29–43). Retrieved 2018-03-27, from http://link.springer.com/10.1007/978-3-319-59536-8{_}3 doi: 10.1007/978-3-319-59536-8_3

Deloitte. (2017). *Blockchain risk management - Risk functions need to play an active role in shaping blockchain strategy* (Tech. Rep.). Retrieved 2018-03-26, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-risk-management.pdf

Devaney, L., & Henchion, M. (2018, may). Who is a Delphi expert'? Reflections on a bioeconomy expert selection procedure from Ireland. *Futures*, *99*, 45–55. Retrieved 2018-06-20, from https://www.sciencedirect.com/science/article/pii/S0016328717302276 doi: 10.1016/J.FUTURES.2018.03.017

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. In *Proceedings of the second international conference on internet-of-things design and implementation* (pp. 173–178). ACM.

Ellervee, A., Matulevicius, R., & Mayer, N. (2017). A Comprehensive Reference Model for Blockchain-based Distributed Ledger Technology. In *Ceur* (pp. 320–333). Retrieved 2018-03-27, from http://ceur-ws.org/Vol-1979/paper-09.pdf

Energy Web Foundation. (2018). *The Energy Web Blockchain.* Retrieved 2018-10-10, from https://energyweb.org/blockchain/

Farrell, M., & Gallagher, R. (2015, sep). The Valuation Implications of Enterprise Risk Management Maturity. *Journal of Risk and Insurance*, *82*(3), 625–657. Retrieved 2018-04-23, from http://doi.wiley.com/10.1111/jori.12035 doi: 10.1111/jori.12035

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access*, 1–1. Retrieved 2018-06-08, from https://ieeexplore.ieee.org/document/8370027/ doi: 10.1109/ACCESS.2018.2842685

Finck, M. (2017, nov). Blockchains and Data Protection in the European Union. *SSRN Electronic Journal*. Retrieved 2018-12-07, from https://www.ssrn.com/abstract=3080322 doi: 10.2139/ssrn.3080322

Garcia, H. (2018). *Decentralizing the charging business for the eMobility Industry (part II).* Retrieved 2018-10-10, from https://medium.com/share-charge/decentralizing-the-charging-business-for-the-emobility-industry-part-ii-6e1b391823e5

Gartner. (2018a). *Gartner IAM Maturity Scale* (Tech. Rep.). Author. Retrieved from https://www.gartner.com/ngw/eventassets/en/conferences/iame13/documents/gartner-identity-access-management-summit-uk-iam-maturity-2018.pdf

Gartner. (2018b). *Internet of Things Defined - Tech Definitions by Gartner.* Retrieved 2018-06-26, from https://www.gartner.com/it-glossary/internet-of-things

Gauba, A. (2018). *Finality in Blockchain Consensus Mechanism Labs Medium.* Retrieved 2018-11-27, from https://medium.com/mechanism-labs/finality-in-blockchain-consensus-d1f83c120a9a

Grey, M. (2017). *Introducing Project Bletchley.* Retrieved 2018-10-29, from https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md

Gupta, S. (2014). *Performance risk mitigation strategies.* Retrieved 2018-08-01, from http://www.quotium.com/performance/performance-risk-mitigation-strategies/

Hasson, F., Keeney, S., & Mckenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing*, *32*(4). doi: 10.1046/j.1365-2648.2000.t01-1-01567.x

Hileman, G., & Rauchs, M. (2017, sep). *2017 Global Blockchain Benchmarking Study.* Retrieved 2018-03-23, from https://ssrn.com/abstract=3040224

Hüner, K. M., Ofner, M., & Otto, B. (2009). Towards a maturity model for corporate data quality management. In *Proceedings of the 2009 acm symposium on applied computing - sac '09* (p. 231). New York, New York, USA: ACM Press. Retrieved 2018-08-01, from http://portal.acm.org/citation.cfm?doid=1529282.1529334 doi: 10.1145/1529282.1529334

Iansiti, M., & Lakhani, K. (2017). The Truth About Blockchain. *Harvard business review*. Retrieved from https://hbr.org/2017/01/the-truth-about-blockchain

IoT Chain. (2017). *IOT Chain: A high-security lite IoT OS* (Tech. Rep.).

ISACA. (2009). *The Risk IT Framework excerpt* (Tech. Rep.). Retrieved 2018-04-06, from http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt{_}fmk{_}Eng{_}0109.pdf

ISO. (2011). *ISO-IEC 27005:2011: Information technology – Security techniques – Information security risk management* (Tech. Rep.). Author. Retrieved from https://www.iso.org/standard/56742.html

Karafiloski, E., & Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. In *17th ieee international conference on smart technologies, eurocon 2017 - conference proceedings* (pp. 763–768). Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University, Skopje, Macedonia. Retrieved from https://www.scopus.com/inward/record.uri?eid=2-s2.0-85029379106{&}doi=10.1109{%}2FEUROCON.2017.8011213{&}partnerID=40{&}md5=ec54b9e5c0320fbaee5702bb88314d3e doi: 10.1109/EUROCON.2017.8011213

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. Retrieved from https://www.scopus.com/inward/record.uri?eid=2-s2.0-85035321551{&}doi=10.1016{%}2Fj.future.2017.11.022{&}partnerID=40{&}md5=2519e8016e9b2f360ee4fecfafc5daba doi: 10.1016/j.future.2017.11.022

King, J. L., & Kraemer, K. L. (1984, may). Evolution and organizational information systems: an assessment of Nolan's stage model. *Communications of the ACM*, *27*(5), 466–475. Retrieved 2018-04-12, from http://portal.acm.org/citation.cfm?doid=358189.358074 doi: 10.1145/358189.358074

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). *Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts* (Tech. Rep.). Retrieved 2018-06-01, from https://eprint.iacr.org/2015/675.pdf

Koteska, B., Karafiloski, E., & Mishev, A. (2017). Blockchain implementation quality challenges: A literature review. In *Ceur workshop proceedings* (Vol. 1938). University SS. Cyril and Methodius, Faculty of Computer Science and Engineering, Rugjer Boshkovikj 16, Skopje, Macedonia. Retrieved from https://www.scopus.com/inward/record.uri?eid=2-s2.0-85030769005{&}partnerID=40{&}md5=5b1c2f3afd44e99a8de6dd1ba36b1b3d

KPMG. (2017, dec). *Blockchain maturity model — KPMG — NL.* Retrieved 2017-12-26, from https://home.kpmg.com/nl/en/home/insights/2017/12/blockchain-maturity-model.html

Kuppinger, M. (2007). *Identity Management Roadmap and Maturity Levels* (Tech. Rep.). Retrieved 2018-10-25, from https://www.kuppingercole.com/files/kuppingerroadmap.pdf

Lahrmann, G., Marx, F., Mettler, T., Winter, R., & Wortmann, F. (2011). Inductive Design of Maturity Models: Applying the Rasch Algorithm for Design Science Research. In (pp. 176–191). Springer, Berlin, Heidelberg. Retrieved 2018-04-22, from http://link.springer.com/10.1007/978-3-642-20633-7{_}13 doi: 10.1007/978-3-642-20633-7_13

Larsson, J. (2018). *Blockchain Disruption in Finance: KYC/AML Blockchain Disruption in Finance Medium.* Retrieved 2018-12-07, from https://medium.com/blockchain-disruption-in-finance/blockchain-disruption-in-finance-kyc-aml-da0d00ef75ae

Lee, S. (2018). *Explaining Directed Acylic Graph (DAG), The Real Blockchain 3.0.* Retrieved 2018-03-27, from https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/{#}45b40c3b180b

LeMahieu, C. (2014). *RaiBlocks: A feeless distributed cryptocurrency network* (Tech. Rep.). Retrieved 2018-03-27, from https://raiblocks.net/media/RaiBlocks{_}Whitepaper{_}{_}English.pdf

Lewenberg, Y., Sompolinsky, Y., & Zohar, A. (2015). Inclusive Block Chain Protocols. In (pp. 528–547). Springer, Berlin, Heidelberg. Retrieved 2018-04-04, from http://link.springer.com/10.1007/978-3-662-47854-7{_}33 doi: 10.1007/978-3-662-47854-7_33

Linstone, H. A., & Turoff, M. (1975). *The Delphi Method : Techniques and Applications.* Retrieved from is.njit.edu/pubs/delphibook/

Maull, R., Godsiff, P., Mulligan, C., Brown, A., & Kewell, B. (2017, sep). Distributed ledger technology: Applications and implications. *Strategic Change*, *26*(5), 481–489. Retrieved from http://doi.wiley.com/10.1002/jsc.2148 doi: 10.1002/jsc.2148

Maxwell, G. (n.d.). *Confidential Transactions.* Retrieved 2018-10-28, from https://elementsproject.org/features/confidential-transactions/investigation

Merchant, N. (2011). *Eight Dangers of Collaboration.* Retrieved 2018-09-25, from https://hbr.org/2011/12/eight-dangers-of-collaboration

Mettler, T. (2011). Maturity assessment models: a design science research approach. *Int. J. Society Systems Science*, *3*(12), 81–98. Retrieved 2018-03-19, from https://www.alexandria.unisg.ch/214426/1/IJSSS0301-0205{%}2520METTLER.pdf

Mettler, T., Rohner, P., & Winter, R. (2010). Towards a Classification of Maturity Models in Information Systems. In D'Atri Alessandro, M. and De Marco, and Braccini Alessio Maria, & and Cabiddu Francesca (Eds.), *Management of the interconnected world* (pp. 333–340). Heidelberg: Physica-Verlag HD.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Annals of internal medicine*, *151*(4), 264–269. Retrieved from http://annals.org/article.aspx?articleid=744664

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System* (Tech. Rep.). Retrieved 2018-03-27, from www.bitcoin.org

NIST. (2012). *Guide for conducting risk assessments* (Tech. Rep.). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf doi: 10.6028/NIST.SP.800-30r1

Nolan, R. (1979). Managing the Crises in Data Processing. *Harvard Business Review*. Retrieved from https://hbr.org/1979/03/managing-the-crises-in-data-processing

Nolan, R. L. (1973, jul). Managing the computer resource: a stage hypothesis. *Communications of the ACM*, *16*(7), 399–405. Retrieved from http://portal.acm.org/citation.cfm?doid=362280.362284 doi: 10.1145/362280.362284

Okoli, C., & Pawlowski, S. D. (2004, dec). The Delphi method as a research tool: an example, design considerations and applications. *Information & Management*, *42*(1), 15–29. Retrieved 2018-04-27, from https://www.sciencedirect.com/science/article/pii/S0378720603001794 doi: 10.1016/J.IM.2003.11.002

Paulk, M., Curtis, B., Chrissis, M., & Weber, C. (1993, jul). Capability maturity model, version 1.1. *IEEE Software*, *10*(4), 18–27. Retrieved 2017-12-23, from http://ieeexplore.ieee.org/document/219617/ doi: 10.1109/52.219617

Pinna, A., & Ruttenberg, W. (2016). *Distributed ledger technologies in securities post-trading Revolution or evolution?* (Tech. Rep.). European Central Bank. Retrieved 2018-03-28, from https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf

Platt, C. (2017). *Of permissions and blockchains... A view for financial markets.* Retrieved 2018-03-27, from https://medium.com/@colin{_}/of-permissions-and-blockchains-a-view-for-financial-markets-bf6f2be0a62

Popov, S. (2017). The Tangle. Retrieved 2018-03-27, from https://iota.org/IOTA{_}Whitepaper.pdf

Pöppelbuß, J., Niehaves, B., Simons, A., & Becker, J. (2011). Maturity Models in Information Systems Research: Literature Search and Analysis. *Communications of the Association for Information Systems*, *29*(29), 505–532. Retrieved from http://aisel.aisnet.org/cais/vol29/iss1/27

Pöppelbuß, J., & Röglinger, M. (2011). What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management. In *Proceedings of the 19th european conference on information systems (ecis).* Retrieved from http://aisel.aisnet.org/ecis2011

Porter, M., & Heppelmann, J. (2014). *How Smart, Connected Products Are Transforming Competition.* Retrieved 2018-09-07, from https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition

RIMS. (2006). *RIMS Risk Maturity Model (RMM) for Enterprise Risk Management* (Tech. Rep.). Risk and Insurance Management Society (RIMS). Retrieved 2018-04-17, from https://www.logicmanager.com/pdf/rims{_}rmm{_}executive{_}summary.pdf

Risk Management Society. (2018). *RIMS Risk Maturity Model.* Retrieved 2018-04-26, from https://www.rims.org/resources/ERM/Pages/RiskMaturityModel.aspx

Rosemann, M., & Bruin, T. (2005, jan). Towards a Business Process Managment Maturity Model. *ECIS 2005 Proceedings*. Retrieved from https://aisel.aisnet.org/ecis2005/37

Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: issues and analysis. *International Journal of Forecasting*, *15*, 353–375. Retrieved from www.elsevier.com

RSA. (2018). *Regulatory and Corporate Compliance Management* (Tech. Rep.). Author. Retrieved 2018-10-29, from https://www.rsa.com/content/dam/en/maturity-model/regulatory-and-corporate-compliance-management-extended.pdf

Santander Innoventures, Oliver Wyman, & Anthemis Group. (2015). *The Fintech 2.0 Paper: rebooting financial services* (Tech. Rep.). Retrieved 2018-04-03, from

http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/jun/The{_}Fintech{_}2{_}0{_}Paper{_}Final{_}PV.pdf

Skulmoski, G. J., Francis Hartman, z. T., & Krahn, J. (2007). The Delphi Method for Graduate Research. *Journal of Information Technology Education*, *6*. Retrieved 2018-04-27, from http://jite.org/documents/Vol6/JITEv6p001-021Skulmoski212.pdf

Smits, D., & Van Hillegersberg, J. (2015). IT Governance Maturity: Developing a Maturity Model using the Delphi Method. Retrieved 2018-03-23, from https://www.knvi.nl/wp-content/uploads/2017/08/Governance-Maturity-Developing-a-Maturity-Model-using-the-Delphi-Method.pdf doi: 10.1109/HICSS.2015.541

Spenkelink, H. (2017). *Blockchain: with great power comes great responsibility - Compact.* Retrieved 2018-02-03, from https://www.compact.nl/articles/blockchain-with-great-power-comes-great-responsibility/

Spilter. (n.d.). *Spilter.* Retrieved 2018-07-18, from https://www.spilter.nl/

Symantec. (2016). *Mirai: what you need to know about the botnet behind recent major DDoS attacks — Symantec Connect Community.* Retrieved 2018-07-23, from https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks

Tableau Software. (2018). *Tableau Desktop.* Retrieved 2018-11-29, from https://www.tableau.com/products/desktop

Van Dijk, F. W., Willem, F., Van Hillegersberg, J., & Daneva, M. (2017). Adopting the Cloud A multi-method approach towards developing a cloud maturity model. Retrieved 2018-04-27, from http://essay.utwente.nl/73075/1/Dijk{_}MA{_}EEMCS.pdf

van der Voort, R., & Spenkelink, H. (2018). Blockchain Maturity Model. In A. Shahim, J. van Praat, P. Harmzen, & R. Matthijsse (Eds.), *Research in it-auditing: A multidisciplinary view* (pp. 47–69). Amsterdam: Vrije Universiteit SBE. Retrieved 2018-05-18, from http://vurore.nl/images/vurore/downloads/publicaties/20180504/RESEARCH-IN-IT-AUDITING.pdf

Walport, M. (2016). *Distributed ledger technology: beyond block chain* (Tech. Rep.). UK Government Office for Science. Retrieved from https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

Wang, H., Chen, K., & Xu, D. (2016). A maturity model for blockchain adoption. *Financial Innovation*, *2*(1), 12. Retrieved from https://link.springer.com/content/pdf/10.1186{%}2Fs40854-016-0031-z.pdfhttp://jfin-swufe.springeropen.com/articles/10.1186/s40854-016-0031-z doi: 10.1186/s40854-016-0031-z

Wieringa, R. (2014). *Design Science Methodology for Information Systems and Software Engineering*. Springer-Verlag Berlin Heidelberg.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on Blockchain technology? - A systematic review. *PLoS ONE*, *11*(10). Retrieved 2018-06-02, from https://www.scopus.com/inward/record.uri?eid=2-s2.0-84991447929{&}doi=10.1371{%}2Fjournal.pone.0163477{&}partnerID=40{&}md5=bbc5d1ac8e2de3e63549e6095dafd424 doi: 10.1371/journal.pone.0163477

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2017, aug). The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *SSRN Electronic Journal*. Retrieved 2018-10-29, from https://www.ssrn.com/abstract=3018214 doi: 10.2139/ssrn.3018214

Appendix A

Evaluations of maturity models

This section will include the detailed evaluation of each maturity model.

A.1 CMMI Development v1.3

A.1.1 Applicability

Origin of the model - Academic; basis in academia of the Software Engineering Institute at Carnegie Melon.
Reliability - Validated; maturity model has been evaluated in many different environments and is validated.
Accessibility - Free/Charged; the 1.3 version of the model is available for free. The newest version is not available for free anymore.
Practicality of recommendations - General Recommendations; they are relatively abstract to apply to a multitude of processes. Appraisals have a higher level of detail. For example the Standard CMMI Appraisal Method for Process Improvement (SCAMPI) is an appraisal method which focuses on identifying improvement opportunities and comparing the organization's processes to CMMI best practices.
Method of application - Certified professionals; there are multiple appraisal methods available that must conform with the a number of published requirements set by the Software Engineering Institute called the Appraisal Requirements for CMMI (ARC). Being appraised by a ARC certified method enables for the most in depth review of processes. Self assessments are also possible but are usually methods to sell an additional more extensive appraisal.
Design mutability - Form and functioning; CMMI is a well established maturity model with many organizations already using it. Elements are easily mutable since there are relatively abstract. They can be easily be applied to existing organizational models.

A.1.2 Design principles

1. ***Basic design principles***

    1.1 **Basic information**

        a) Application domain:
            Organizations?
        b) Prerequisites of applicability:

Not mentioned

c) Purpose of use:
Descriptive, Prescriptive, Comparative; Guide process improvement across a project, division, or an entire organization

d) Target group:
Organizations in General

e) Class of entities under investigation:
Processes within organizations

f) Differentiation from related maturity models
Differences between the different versions of the model explained. Evolution from CMM to CMMi explained. Differentiation with Crosby's model explained.

g) Design process and extend of empirical validation:
Literature research; research on product quality. Each model extensively reviewed by large panel of experts in between each version

1.2 **Definition of central constructs related to maturity and maturation**

a) Maturity and dimensions of maturity
Definition of maturity not given.

b) Maturity levels and maturation paths:
Levels and paths clearly defined

c) Available levels of granularity of maturation:
Granularity clearly defined

d) Underpinning theoretical foundations with respect to evolution and change:
Basis in Nolan's stage model and Crosby's Quality maturity grid

1.3 **Definition of central constructs related to the application domain**

Central constructs are explained in part 1 of the model

1.4 **Target group-oriented documentation**

Available on CMMI institute website

2. ***Descriptive design principles***

2.1 **Intersubjectively verifiable criteria for each maturity level and level of granularity**

Criteria are clearly defined in the CMMI documentation

2.2 **Target-group oriented assessment methodology**

a) Procedure model:
Within ARC documentation

b) Advice on the assessment of criteria:
Within ARC documentation

c) Advice on the adaption and configuration of criteria:
Within ARC documentation

d) Expert knowledge from previous application:
Available from appraisal organizations or select appraisals of companies available on CMMI website

3. ***Prescriptive design principles***

3.1 **Improvement measures for each maturity level and level of granularity**

Included in CMMI documentation using specific goals which can be attained to reach the level.

3.2 **Decision calculus for selecting improvement measures**

a) Explication of relevant objectives:
Defined in generic goals

b) Explication of relevant factors of influence:
Not included

c) Distinction between an external reporting and an internal improvement perspective:
Not included

3.3 **Target group-oriented decision methodology**

a) Procedure model:
Not included

b) Advice on the assessment of variables:
Not included

c) Advice on the concretization and adaption of the improvement measures:
Not included

d) Advice on the adaption and the configuration of the decision calculus:
Not included

e) Expert knowledge from previous application:
Available on appraisal website

A.2 Risk Maturity Model

A.2.1 Applicability

Origin of the model - Practitioner-based; created by Logicmanager in collaboration with the Risk and Insurance Management Society (RIMS)
Reliability - Validated; Research at Queens university found that organizations with higher maturity scores realized an increased valuation premium of up to 25% (Farrell & Gallagher, 2015). Maturity model has been used by over 2000 organizations across multiple industries. It has be verified at these industries but no instances of validation of the model has been found.
Accessibility - Charged; A self assessment of the model is available for free online. The full guidelines are available at a cost but a limited executive summary of the guidelines are available for free.
Practicality of recommendations - General recommendations; Results of assessment can be compared to the guidelines to create a plan for improving processes.
Method of application - Self-assessment; a self assessment is available for free to evaluate the risk management processes.
Design mutability - Form; The maturity model has its basis in CMMI, when this model is already used within the organization it is easily adaptable. The functioning of the model is not easily adaptable since the self assessment cannot be adapted.

A.2.2 Design principles

1. ***Basic design principles***

1.1 **Basic information**

a) Application domain:
Organizations

b) Prerequisites of applicability:
Not mentioned

c) Purpose of use:
Descriptive, Prescriptive, Comparative; Provide reports for standards, better their risk management processes, compare with other businesses.

d) Target group:
Risk and governance professionals

e) Class of entities under investigation:
Risk management processes

f) Differentiation from related maturity models
No differentiation between other maturity models. Only comparisons with existing risk frameworks. The RMM aims to combine the frameworks.

g) Design process and extend of empirical validation:
Design process not specified.

1.2 **Definition of central constructs related to maturity and maturation**

a) Maturity and dimensions of maturity
Definition of maturity not given.

b) Maturity levels and maturation paths:
Levels and paths clearly defined

c) Available levels of granularity of maturation:
Granularity clearly defined, per attribute there are separate key drivers that drive the maturity level of that attribute.

d) Underpinning theoretical foundations with respect to evolution and change:
Basis in existing risk frameworks and CMMI.

1.3 **Definition of central constructs related to the application domain**

Constructs are explained in the definition of terms within the executive summary of the model.

1.4 **Target group-oriented documentation**

Available on RIMS website

2. ***Descriptive design principles***

2.1 **Intersubjectively verifiable criteria for each maturity level and level of granularity**

Criteria are not published in executive summary

2.2 **Target-group oriented assessment methodology**

a) Procedure model:
Not a full procedure model, basic instructions as to how to do the self assessment and what to do with the results

b) Advice on the assessment of criteria:
Within self assessment

c) Advice on the adaption and configuration of criteria:
Not included

d) Expert knowledge from previous application:
Case studies included on the RIMS website under resources

3. ***Prescriptive design principles***

3.1 **Improvement measures for each maturity level and level of granularity**

Specific improvement measures are not given. Key drivers are mentioned but not how to improve these key drivers. There are "well-managed guidelines" which can be used to develop an action plan to improve the maturity of the risk management program.

3.2 **Decision calculus for selecting improvement measures**

a) Explication of relevant objectives:
Not included

b) Explication of relevant factors of influence:
Not included

c) Distinction between an external reporting and an internal improvement perspective:
Not included

3.3 **Target group-oriented decision methodology**

a) Procedure model:
Not included

b) Advice on the assessment of variables:
Not included

c) Advice on the concretization and adaption of the improvement measures:
Not included

d) Advice on the adaption and the configuration of the decision calculus:
Not included

e) Expert knowledge from previous application:
Not included

A.3 IT Capability Maturity Framework Risk Management

A.3.1 Applicability

Origin of the model - Academics; created by the Innovation Value Institute of the National University of Ireland Maynooth.
Reliability - Verified; The IT CMF has been created with a design science methodology, starting from the framework and filling in the specific critical capabilities (like risk management (RM)) in different research cycles. The RM critical capability (CC) by itself is, according to the initial research, not validated thoroughly. In the presenting paper ((Carcary, 2013)) it is noted future research will involve testing the model with case studies and assessments. Although some case studies have been found utilizing the IT CMF, these do not explicitly mention the RM CC. It is possible this research has been carried out but not published or presented at a conference.
Accessibility - Charged; the complete model is not available for free. The complete model is presented in a book that is available for sale.
Practicality of recommendations - Specific improvement activities; the recommendations are problem-specific. The recommendations from an assessment can be implemented within the organization according to the IT Capability Improvement Programme. This is a paid program which guides an

organization to improve their capabilities.
Method of application - Third-party assisted; there are multiple assessments are available each tailoring to a specific purpose. There is no assessment available for specific evaluation of IT risks. The assessments can however be tailored to specific needs, this may also be specific to IT risk management.
Design mutability - Form and functioning; the IT CMF acts as a unifying framework for other specific frameworks already in the organization. Therefor it is easily integrated into an organization.

A.3.2 Design principles

1. ***Basic design principles***

   1.1 **Basic information**

   a) Application domain:
      Organizations?
   b) Prerequisites of applicability:
      Not mentioned
   c) Purpose of use:
      Descriptive, Prescriptive; Provide an evaluation of the current state of IT management within an organization and provide improvement measures to improve it.
   d) Target group:
      IT management professionals
   e) Class of entities under investigation:
      IT related processes within organizations
   f) Differentiation from related maturity models:
      Comparison with CMMI and Nolan's stage theory.
   g) Design process and extend of empirical validation:
      Literature research; identifying indicators for IT management

   1.2 **Definition of central constructs related to maturity and maturation**

   a) Maturity and dimensions of maturity
      Maturity is defined along with the different dimensions of maturity.
   b) Maturity levels and maturation paths:
      Maturity levels are clearly defined based on CMMI.
   c) Available levels of granularity of maturation:
      Granularity is based on critical capabilities.
   d) Underpinning theoretical foundations with respect to evolution and change:
      Basis in Nolan's stage model, CMMI, Crosby's Quality maturity grid

   1.3 **Definition of central constructs related to the application domain**

   Specific IT related constructs are well defined.

   1.4 **Target group-oriented documentation**

   Available on the Innovation Value Institute website

2. ***Descriptive design principles***

   2.1 **Intersubjectively verifiable criteria for each maturity level and level of granularity**

   Criteria available in the full IT CMF model

2.2 **Target-group oriented assessment methodology**

a) Procedure model:
Different assessments possible based on the needs of the organization

b) Advice on the assessment of criteria:
Advice given using a 'capability improvement program'

c) Advice on the adaption and configuration of criteria:
Advice given using a 'capability improvement program'

d) Expert knowledge from previous application:
Use cases available on the IVI website

3. ***Prescriptive design principles***

3.1 **Improvement measures for each maturity level and level of granularity**
Unknown, Possibly included in the 'Capability Improvement Program'

3.2 **Decision calculus for selecting improvement measures**

a) Explication of relevant objectives:
Included in the 'Capability Improvement Program' in the Discover phase

b) Explication of relevant factors of influence:
Included in the 'Capability Improvement Program' in the Discover phase

c) Distinction between an external reporting and an internal improvement perspective:
Included in the 'Capability Improvement Program' in the Discover phase

3.3 **Target group-oriented decision methodology**

a) Procedure model:
Included in the 'Capability Improvement Program' in the Design phase

b) Advice on the assessment of variables:
Included in the 'Capability Improvement Program' in the Design phase

c) Advice on the concretization and adaption of the improvement measures:
Included in the 'Capability Improvement Program' in the Design phase

d) Advice on the adaption and the configuration of the decision calculus:
Unknown, Possibly included in the 'Capability Improvement Program'

e) Expert knowledge from previous application:
Unknown, Possibly included in the 'Capability Improvement Program'

A.4 Maturity Model for Blockchain Adoption

A.4.1 Applicability

Origin of the model - Academics; created by Wang et al. (2016).
Reliability - Untested; The model is not validated or verified in any way.
Accessibility - Free; The model is published under open access at Springer.
Practicality of recommendations - General recommendations; General on blockchain technology
Method of application - None; There is not a method described to apply this model.
Design mutability - Form; The levels of maturity are defined according to CMMI. Other than this it is a separate model which provides no way of integrating or assessing technologies.

A.4.2 Design principles

1. ***Basic design principles***

   1.1 **Basic information**

   a) Application domain:
   Organizations?

   b) Prerequisites of applicability:
   Not mentioned

   c) Purpose of use:
   Descriptive; mainly used as a description of the current state of blockchain technology

   d) Target group:
   Organizations thinking about adopting blockchain

   e) Class of entities under investigation:
   Blockchain technology

   f) Design process and extend of empirical validation:
   No well established design process. Taxonomy of model made from non-cited stage definitions based on CMM. Model created with this taxonomy and one source which is an interview within IEEE spectrum.

   1.2 **Definition of central constructs related to maturity and maturation**

   a) Maturity and dimensions of maturity
   Definition of maturity not given.

   b) Maturity levels and maturation paths:
   Levels defined in taxonomy

   c) Available levels of granularity of maturation:
   No granularity

   d) Underpinning theoretical foundations with respect to evolution and change:
   Based on CMM

   1.3 **Definition of central constructs related to the application domain**
   Central constructs not explained

   1.4 **Target group-oriented documentation**
   Short paper available assessing the current state of blockchain technology.

2. ***Descriptive design principles***

   2.1 **Intersubjectively verifiable criteria for each maturity level and level of granularity**
   Criteria for maturity levels mentioned in general taxonomy but it is not applicable to all indicators.

   2.2 **Target-group oriented assessment methodology**

   a) Procedure model:
   Not included

   b) Advice on the assessment of criteria:
   Not included

   c) Advice on the adaption and configuration of criteria:
   Not included

d) Expert knowledge from previous application:
Not included

3. ***Prescriptive design principles***

3.1 **Improvement measures for each maturity level and level of granularity**
Not included

3.2 **Decision calculus for selecting improvement measures**
Not included

a) Explication of relevant objectives:
Not included

b) Explication of relevant factors of influence:
Not included

c) Distinction between an external reporting and an internal improvement perspective:
Not included

3.3 **Target group-oriented decision methodology**

a) Procedure model:
Not included

b) Advice on the assessment of variables:
Not included

c) Advice on the concretization and adaption of the improvement measures:
Not included

d) Advice on the adaption and the configuration of the decision calculus:
Not included

e) Expert knowledge from previous application:
Not included

A.5 KPMG Blockchain Maturity Model

A.5.1 Applicability

Origin of the model - Academics; created by van der Voort and Spenkelink (2018).
Reliability - Verified; the model is verified at a financial services organization. It has been used in multiple other projects involving blockchain technology ranging from other financial services to non-profit organizations. The model itself is created with multiple
Accessibility - Charged; the model is not available for free. An assessment can be done by KPMG.
Practicality of recommendations - Specific improvement activities; recommendations are very specific as to what to improve to an application to reach a desired maturity level.
Method of application - Third-party assisted; the model is applied through an assessment that is administered by KPMG.
Design mutability - Form and functioning; The model is based on CMMI and elements are included of multiple risk management frameworks. The model is also applicable to multiple applications since the assessment is administered by KPMG which can change recommendations based on the application behind it.

A.5.2 Design principles

1. ***Basic design principles***

1.1 **Basic information**

a) Application domain:
Organizations

b) Prerequisites of applicability:
Not mentioned

c) Purpose of use:
Descriptive; Measure IT maturity on IT risks associated with the use of DLT in organizations.

d) Target group:
Organizations looking at implementing a DLT and DLT providers

e) Class of entities under investigation:
IT risks of DLT

f) Design process and extend of empirical validation:
Design science research. Extensive literature research with verification with a case study.

1.2 **Definition of central constructs related to maturity and maturation**

a) Maturity and dimensions of maturity
Definition of maturity not given in available literature

b) Maturity levels and maturation paths:
Levels based on CMMI. Maturation paths same as CMMI.

c) Available levels of granularity of maturation:
Granularity based on the different maturity levels for different risk areas

d) Underpinning theoretical foundations with respect to evolution and change:
Not clear from available literature but based on the CMMI model.

1.3 **Definition of central constructs related to the application domain**

Central constructs are explained clearly. Differences between various DLTs are explained clearly.

1.4 **Target group-oriented documentation**

Target group documentation is available although not very extensive.

2. ***Descriptive design principles***

2.1 **Intersubjectively verifiable criteria for each maturity level and level of granularity**

No access to entire model, but parts of model have clear criteria for each maturity level based on the assessment.

2.2 **Target-group oriented assessment methodology**

a) Procedure model:
Model is assessed with the help of KPMG, the process of assessment is explained but not in much detail.

b) Advice on the assessment of criteria:
It is a self assessment but it is verified by KPMG consultants

c) Advice on the adaption and configuration of criteria:
Criteria are not easily adapted since there is only an assessment available

d) Expert knowledge from previous application:
Sharing of limited use case information.

3. ***Prescriptive design principles***

3.1 **Improvement measures for each maturity level and level of granularity**

Measures not given but advice as how to improve is given during the assessment carried out by KPMG.

3.2 **Decision calculus for selecting improvement measures**

a) Explication of relevant objectives:
In the results of the assessment weaker risk areas are highlighted and improvement advice is given.

b) Explication of relevant factors of influence:
Not clear from available documentation

c) Distinction between an external reporting and an internal improvement perspective:
Model is aimed at internal improvement.

3.3 **Target group-oriented decision methodology**

a) Procedure model:
No procedure model available

b) Advice on the assessment of variables:
Not included

c) Advice on the concretization and adaption of the improvement measures:
Included in the advice of KPMG

d) Advice on the adaption and the configuration of the decision calculus:
Not included

e) Expert knowledge from previous application:
Not clear from documentation, sharing of limited use case information.

Appendix B

Literature study results

This appendix presents the studies that have been identified through the literature study

B.1 Included papers

ID	Title	Authors	Publication	Publication type	Year
S01	Cybersecurity Challenges and Opportunities in the New ”Edge Computing + IoT” World	Pan et al.	ACM	Workshop	2018
S02	Towards an Optimized BlockChain for IoT	Dorri et al.	ACM	Conference	2017
S03	Overcoming Limits of Blockchain for IoT Applications	Buccafurri et al.	ACM	Conference	2017
S04	Peer to Peer for Privacy and Decentralization in the Internet of Things	Conoscenti et al.	IEEE	Conference	2017
S05	Blockchain: A game changer for securing IoT data	Singh et al.	IEEE	Forum	2018
S06	Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard	Fabiano	IEEE	Conference	2017
S07	Towards using blockchain technology for IoT data access protection	Rifi et al.	IEEE	Conference	2017
S08	Blockchains for business process management - Challenges and opportunities	Mendling et al.	ACM	Article	2018
S09	Where Is Current Research on Blockchain Technology?A Systematic Review	Yli-Huumo et al.	PLoS ONE	Article	2016
S10	Towards better availability and accountability for IoT updates by means of a blockchain	Boudguiga et al.	IEEE	Conference	2017
S11	Blockchain implementation quality challenges: A literature review	Koteska et al.	CEUR	Conference	2017
S12	Fintech in the Exchange Industry: Potential for Disruption?	Geranio	Masaryk University Journal of Law and Technology	Article	2017
S13	Risk Modelling of Blockchain Ecosystem	Kabashkin	Springer	Conference	2017
S14	To Blockchain or Not to Blockchain: That Is the Question	Gatteschi et al.	IEEE	Magazine Article	2018
S15	An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends	Zheng et al.	IEEE	Conference	2017
S16	Blockchain exhumed	Patel et al.	IEEE	Conference	2017

ID	Title	Authors	Publication	Publication type	Year
S17	Validation and Verification of Smart Contracts: A Research Agenda	Magazzeni et al.	IEEE	Magazine Article	2017
S18	LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy	Dorri et al.	arxiv	Preprint	2017
S19	Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues	Yeow et al.	IEEE	Article	2017
S20	From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues	Dai et al.	IEEE	Conference	2017
S21	IoT and Blockchain Convergence: Benefits and Challenges	Banafa	IEEE	Newsletter	2017
S22	Blockchain-Based Security Solutions for IoT Systems	Pulkkis et al.	Wiley	Book	2018
S23	Blockchains and smart contracts for the internet of things	Christidis et al.	IEEE	Article	2016
S24	Blockchain for the Internet of Things: A systematic literature review	Conoscenti et al.	IEEE	Conference	2016
S25	Development of distributed ledger technology and a first operational risk assessment	Milkau et al.	The Capco Institute	Journal	2016
S26	Trusting records: is Blockchain technology the answer?	Lemieux	Emerald insight	Journal	2016
S27	Blockchain technology: Beyond bitcoin	Crosby et al.	Berkley	Journal	2016
S28	Blockchain Maturity Model	van der Voort et al.	Vrije Universiteit SBE	Bundle	2018
S29	Blockchain risk management - Risk functions need to play an active role in shaping blockchain strategy	Deloitte	Deloitte	Report	2017
S30	Missing link - Navigating the disruption risks of blockchain	Lageschulte et al.	KPMG	Report	2016
S31	Three Risks to Assess as Your Company Considers Blockchain	Hogan	Bradley	Article	2017
S32	A Review on the Use of Blockchain for the Internet of Things	Fernandez-Carames et al.	IEEE	Article	2018

B.2 Consolidated risks from literature

Category	Description	Corresponding S#
Strategic Risks		
Advantages of early adoption	Participants of early networks have certain advantages. This can manifest in a lower effort to participate in the network or having the network infrastructure be designed to perfectly fit the organisation.	S13
Application limitations due to early adoption	A choice in platform to create an application on can pose limitations in terms of functionality in a later stage.	S29
Resistance to culture change	Participants in company/network may be resistant to changes to current infrastructure	S16
Vendor risks	With blockchain as a service solutions trust must be placed in the vendor providing the service. One should carefully select vendors and ensure that proper contract provisions are in place to appropriately transfer risk to them.	S31
High initial costs	Costs of setting up system is expensive due to no ready-to-order systems available and expensive hardware.	S16, S21, S22, S27
DLT participants	It is possible that not all participants of the system have the same benefit. When this is the case a participant may pull out rendering the system broken.	
Operational Risks		
Data accuracy	Data that is onboarded onto the blockchain should be accurate.	S28, S32
Data availability	Data that is used in the blockchain, for example Oracles, should be continuesly available	S14, S28, S29, S32
Data confidentiallity	Data that is put into transactions may be open to anyone, this includes metadata. This metadata can be used to trace back critical business processes.	S08, S11, S14, S23, S24, S32
Key management	When a private key is lost or stolen this can lead to loss of access to system or stolen assets.	S13, S20, S26, S29, S30, S31, S32

Category	Description	Corresponding S#
Authorization management	Authorization of users to access system should be managed properly. High privilage users can promote changes in system	S04, S09, S28
Change management	Inproper change managment can lead to forks in the DLT. It can also lead to some participants' system not working due to integration problems	S28, S32
System abuse	The DLT may be rendered unusable because of abuse of the system due to selfish mining, centralization of mining power, 51% attacks.	
Infrastructure development	Infrastructural issues due to insufficient knowledge on technology	S21
Legacy intergration	System may not integrate properly with legacy systems causing system outages/continuity risks	S12, S16, S28, S30, S32
Support management	When the system is introduced, who is responsible for support of the system?	
Legal risks		
Compliance with legislation	Application may not be compliant with current legislation regarding privacy (GDPR) or other legislation	S06, S32
Changes in legislation	Changes in legislation may render the system inoperable	S16, S21, S22, S27, S32
Legal enforcability	Smart contracts may not be legally enforcable	S23, S25, S29, S32
Handling unexpected outcomes (bounded rationality)	Not all outcomes are known before the creation of a contract. Provisions should be in place to deal with uncertain outcomes	S25, S29
Security risks		
IoT device security	Compromises in IoT device can lead to stolen user data or private keys	S01, S02, S18, S32
DLT infrastructure security	A variance of attacks can compromise DLTs causing them to either cease to exist or compromise their integrity	S13, S15, S16, S20, S24, S26, S32
Cloud storage security	Privacy sensitive data may be accessed through centralized cloud storage	S04, S32

Category	Description	Corresponding S#
Data provider compromised	Compromises in data provider for DLT (Oracles) can lead to system malfunction, for example firing smart contracts when not intended.	S14, S29, S28
Technology risks		
IoT device limitations	Various limitations on IoT device causes some DLT to not function properly.	S02, S03, S07, S09, S10, S18, S21, S22, S32
DLT limitations	Some DLT protocols have poor scalability, high latency, high power usage, high storage needed and high costs for mining hardware	S02, S04, S07, S08, S09, S13, S14, S15, S16, S18, S19, S21, S27, S32
Low processing power of IoT devices	IoT devices usually have low processing power and are not able to run some processes.	
Low storage capacityof IoT devices	IoT devices usually have low storage space which restricts the uses of some DLT due to DLT size.	
Low battery capacity of IoT devices	IoT devices usually have low battery capacity which might restrict the uses of some DLT due to high amount of power used for P2P communications.	
Low bandwidth of IoT devices	IoT devices usually only have a restricted bandwidth to work with, this creates issues for DLTs with large transaction/block sizes	

Appendix C

Delphi Study Surveys

This appendix contains the full surveys as presented to the participants of the Delphi study. The questions will be highlighted in bold text and the answer options in italic.

C.1 Survey 1

Thank you for participating in this study. This is the first survey in a number of four total surveys. At the end of these surveys the goal is to create a comprehensive list of IT risks of DLT for IoT, divided up into several risk areas and ranked based on importance. From this information a maturity model will be created which can be used to evaluate the IT risks of DLT applcations with a focus on IoT.

This first survey will focus on gathering information on the IT risks associated with DLT and dividing these risks up in multiple risk areas. During a literature study a number of risks have already been identified. Please only see these risks as proposals and feel free to addapt these risks and add new risks that you feel are not included. In order to give some structure to the list a number of risk areas have been included as well. These risk areas are again not final and your opinion on them will be asked in the second part of this survey.

The answers from the second and third part of the survey that are given by other participants will be anonymised and visible to all the participants. Use these answers to guide your own and feel free to comment on these answers. If, during the course of the suvery, you run into any trouble with the survey or if you have any questions please let me know.

During the period that the survey is open it is always possible to log in and add additional answers or respond to other answers. It is also possible to fill out the survey in multiple sittings.

The deadline for filling in this survey is 08-07-2018.

C.1.1 Part 1 - Introductory questions

In this section a number of questions will be asked to gather some background information on the demographic of the panel. These will include questions about your company or university, function and your connection with blockchain and IoT.

The answers to these questions will only be visible to the surveyor and will not be shown to other participants of the panel.

What is the sector of industry your company/research is focused on?

For example: Manufacturing, Automotive, Transport, Academics, ...

Answer option: textbox.

What is your focus/function within the company or your research?

What is your function in the company or focus in your reseach and it's connection with Blockchain and IoT?

Answer option: textbox.

What is your personal experience with DLT and IoT?

Do you have any experience with Distributed Ledger Technology or Internet of Things outside of your company or research?

Answer option: textbox.

C.1.2 Part 2 - Identifying IT Risks

This section will contain a number of questions to identify the different IT risks facing blockchain applications specifically connected with IoT. A number of answers have been added already based on a literature review conducted by the surveyer. However, this list is not yet complete. The field of research is still young and it is likely that many IT risks facing these applications have not yet been identified by researchers.

The following definition for IT risks is used as defined by ISACA: IT risks: "The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise."

The risks have been divided up into five risk areas, these areas have been derived by searching for common themes within the complete list of risks. The description of each risk area is given with each question. The definitions and the completeness of the risk areas can be discussed in the next section of this survey.

This section is aimed at creating a large list of risks. Every participant can see the risks added by other participants which might spark ideas for additional risks. Therefor I invite you to look through each list thoroughly to see if you have any risks to add.

In order to keep the list of definitions clear for everyone to read, please add new risks in the following format: "Risk" - "Definition"

Strategic risks

Definition: Risks involving strategic decisions by management surrounding DLT about the organizations' objectives.

Answer option: textbox.

Operational risks

Definition: Risks involving the failure of one of the processes surrounding DLT within the organization. *Answer option: textbox.*

Technology risks

Definition: Risks involving the failure or limitation of DLT or IoT technology which disrupts the organization.

Answer option: textbox.

Security risks

Definition: Risks involving the security of DLT and associated technologies.

Answer option: textbox.

Legal risks

Definition: Risks involving the legal challenges surrounding DLT which can have an influence on the organization.

Answer option: textbox.

C.1.3 Part 3 - Identifying IT Risk areas

Within this section it is possible to provide feedback on the risk areas as defined in the previous section. The categories have been formed by grouping IT Risks under a common theme as found in literature. As a reminder, the following definition for IT risks is used:

IT risks: "The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise."

In the following questions you will be asked to rate each risk category and its definition in two separate questions. Please include some feedback supporting your rating or suggesting an alternate definition. At the end of this category you will be able to provide your own proposal for risk areas if you choose to do so.

Risk area definitions

This question relates to the definitions of the risk areas as listed below. Press on the 'i' icon for the definition of the risk area. Please rate your satisfaction with the definitions of the risk area's.

In the next question you will be able to suggest different definitions for the different risk areas.

Answer option: Five five-point likert style questions rating level of agreement on each definition

Risk area definitions

In case the definitions defined in the previous questions were inaccurate, please suggest an alternative definition for the risk area.

If you agree with the definitions from the previous section you can leave this question blank.

Answer option: textbox.

Risk areas completeness

Do you agree with the different risk area's as defined below? If you do not agree with these risk areas or if you would like to suggest additional ones please indicate your alternative list in the comment box below. These will be taken into account in the next survey round.

If someone else already suggested an alternative list with which you agree, please copy/paste this list in your own comment box.

Please provide a complete list of risk area's when indicating alternative additional areas. Format the list as follows: 1: "First risk area name" - "Description", 2: "Second risk area name" - "Description", etc. Unfortunately it is not possible to use linebreaks (enters) in the comment box.

Five-point likert style question rating level of agreement

C.1.4 Final page

Thank you for filling out the survey. If you are interested in how other participants enter the survey you can always check back before the deadline at 08 July at 23:59. It is always possible to change your own answers before the deadline.

The next survey will be sent out on the 16th of July and will contain also a summary of the responses to this survey. If in the meantime you have any questions or comments, please let me know at j.vermeij-1@student.utwente.nl or fixed-term.jaap.vermeij@de.bosch.com.

C.2 Survey 2

This is the second round of the Delphi study for the creation of an IT risk maturity model. Thank you for the great response in the previous round where some new risks have been identified which are not mentioned in literature yet. Based on the previous round the structure of the model has been changed. A new layer of risk areas has been added and a new distinction has been made in the high-level risk areas. In the next part more information about this change is given.

This round will focus on gathering feedback on the new risk areas and creating a list of risks for inclusion in the model. In the first part, the new risk areas are explained and again feedback will be asked on the different definitions and the completeness of the risk areas. In the second part, the list of risks will be presented which were identified in the previous round. These risks will be rated for measurement by the model as either must stay, can go or either way.

In the previous round there were some issues with the questions that rated risk areas. These issues have been passed on to the creator of the survey software but sadly no fix is found yet. The issues seemed to only affect internet explorer users. This survey contains for a large part a similar format of questions. If issues arise when filling in the survey please try it also on a different browser if possible. If this is not possible please let me know.

It has been decided not to rate the risks during this round as this would lead to a too large survey. Instead, the rating of the risks will be pushed to the next round.

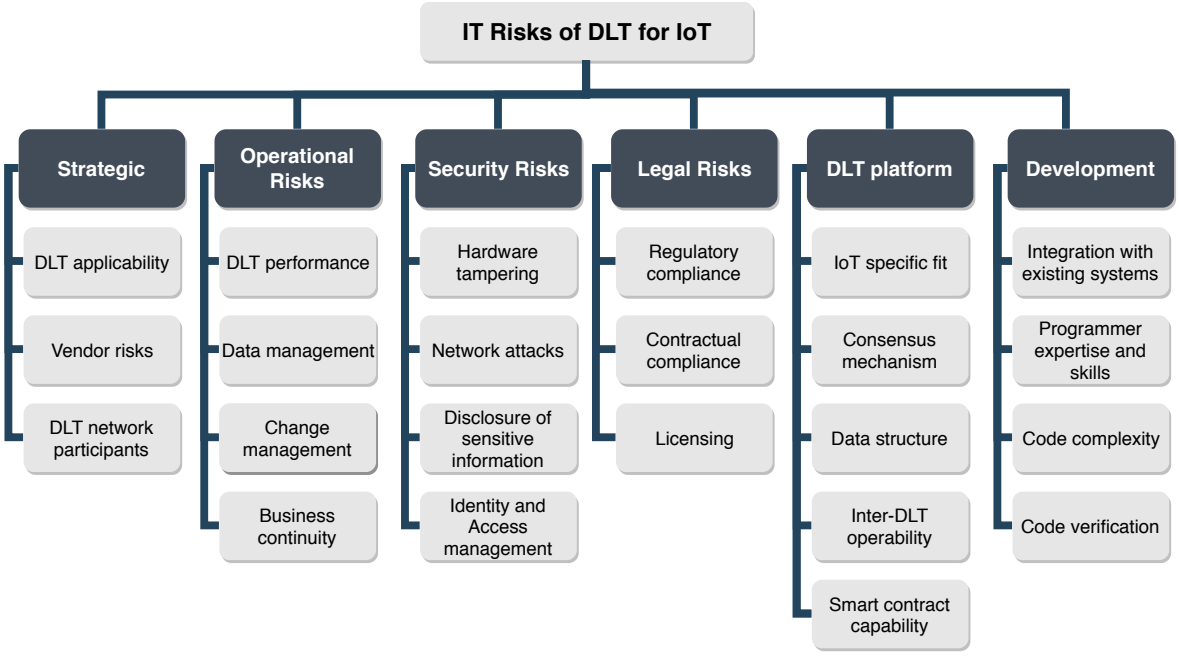

Figure C.1: Redefined two layer model with high- and low-level risk areas

The deadline for filling in this survey will be in two weeks on Friday 27-07-2018.

C.2.1 Part 1 - Redefined Risk Areas

Some of the comments from the previous round showed that the different risk areas have some room for improvement. They overlapped on some parts and are a bit too broad to create good insights. Based on these comments and other suggestions, the risk areas have been redefined to create less overlap and to be able to provide more insights. In order to achieve this, a new layer has been added to the model. This layer is more specific in order to gain more insights in specific DLT related risks. Furthermore, this layer aims to create a clearer divide between the high-level risk areas. The new structure is shown in the picture in the first part of this section, the layer in blue are the high level risk areas, the grey are lower level risk areas.

The specific risks as defined in the previous round will be grouped under these gray lower-level risk areas. This part will focus on the new structure of the risk areas. In the next part the consolidated list of risks collected in the previous round will be presented to be rated for inclusion or exclusion.

Strategic

Please rate your satisfaction with the definition of the strategic risk area and its sub risk areas, defined as:

1. Strategic: Risks arising from strategic decisions surrounding the choice for a DLT and the partners in the network.
2. DLT applicability: Risks arising from poor fit of DLT to the use case.
3. Vendor risks: Risks arising from the choice in DLT platform vendor.
4. Network participants: Risks arising from the choice in DLT network participants.

Please rate your satisfaction with these risk areas and motivate your choice in the comment box.

Five-point likert style question rating level of agreement and mandatory comment box for motivation.

Operational

Please rate your satisfaction with the definition of the operational risk area and its sub risk areas, defined as:

1. Operational: Risks arising from inadequate or failed processes, people or systems surrounding the DLT application.
2. DLT performance: Risks arising from poor performance of DLT.
3. Data management: Risks arising from data management surrounding the DLT.
4. Change management: Risks arising from change management surrounding the DLT.
5. Business continuity: Risks arising from business continuity plans surrounding the DLT.
6. Use of DLT by end users: Risks arising from the use of DLT by end users.

Please rate your satisfaction with these risk areas and motivate your choice in the comment box.

Five-point likert style question rating level of agreement and mandatory comment box for motivation.

Security

Please rate your satisfaction with the definition of the security risk area and its sub risk areas, defined as:

1. Security: Risks arising from security incidents surrounding the DLT and IoT devices.
2. Hardware tempering: Risks arising from individuals tempering with hardware to gain access to network.
3. Software tempering: Risks arising from individuals tempering with software to gain access to network.
4. Disclosure of sensitive information: Risks arising from the unintentional disclosure of sensitive information from either the business or customers.
5. Identity and access management: Risks arising from idenity and access management of participants on the DLT.

Please rate your satisfaction with these risk areas and motivate your choice in the comment box.

Five-point likert style question rating level of agreement and mandatory comment box for motivation.

Legal

Please rate your satisfaction with the definition of the legal risk area and its sub risk areas, defined as:

1. Legal: Risks arising from legal challenges surrounding the DLT application.
2. Regulatory compliance: Risks arising from regulation surrouding DLT.
3. Contractual compliance: Risks arising from contractual agreements between parties using the DLT application.
4. Software licensing: Risks arising from the licensing form of the used DLT in the application.

Please rate your satisfaction with these risk areas and motivate your choice in the comment box.

Five-point likert style question rating level of agreement and mandatory comment box for motivation.

Development

Please rate your satisfaction with the definition of the development risk area and its sub risk areas, defined as:

1. Development: Risks arising during the development of the DLT application.
2. Integration with existing systems: Risks arising from the integration of the DLT application with existing systems in the organisation.
3. Programmer expertise and skills: Risks arising from the lack of programmer expertise and skills with programming DLT related elements.
4. Code verification: Risks arising from the difficulty in verifying code written for DLT related elements.

Please rate your satisfaction with these risk areas and motivate your choice in the comment box.

Five-point likert style question rating level of agreement and mandatory comment box for motivation.

DLT Platform

Please rate your satisfaction with the definition of the DLT platform risk area and its sub risk areas, defined as:

1. DLT platform: Risks arising from the limitations of a chosen DLT platform.
2. IoT specific fit: Risks arising from IoT specific requirements of a DLT platform like scalability and low CPU usage.
3. Consensus mechanism: Risks arising from the chosen consensus mechanism used in the DLT application.
4. Data structure: Risks arising from the used data structure (i.e. Blockchain, DAG, combination...)

5. Smart contract capability: Risks arising from the smart contract capabilities of the platform.
6. Inter-DLT operability: Risks arising from the interoperability of the DLT platform with other DLT networks.

Please rate your satisfaction with these risk areas and motivate your choice in the comment box.

Five-point likert style question rating level of agreement and mandatory comment box for motivation.

Additional comments

Do you have any additional comments regarding the redefined risk areas? These comments will only be visible to the surveyor.

Non-mandatory open text box

C.2.2 Part 2 - Rating risks

This part focusses on deciding which risks the model will cover and will not be covered. The only possibilities will be to include, either way or exclude the risks. The list that will be presented will include risks that have been collected during the previous round and either rewritten or consolidated under other risks. While these risks may be valid for many DLT applications, their abstration level was either too high or too low.

Deciding the abstraction level that creates the most value is difficult. The number of imaginable risks is infinite if you combine all the possible scenarios, and ofcourse infinite lists cannot be used for maturity modelling. Therefor a choice in risks and generalizations has been made. If you believe there are risks that have not been included or do not fall under one of the presented risks, please add these risks at the end of the round.

In order to keep this questionaire clear, each question will focus on one of the high-level risk areas with distinction made within the question as to which low level risk area the risk applies to.

Strategic

Please note if you would like to include or exclude the listed risks from the strategic high level-risk area. The numbers in front of the risk correspond to the following low level risk areas:

1. DLT applicability
2. Vendor choice
3. DLT network participants

Operational

Please note if you would like to include or exclude the listed risks from the strategic high-level risk area. The numbers in front of the risk correspond to the following low level risk areas:

1. DLT performance
2. Data management

Parts	Description
1. DLT not providing expected benefits	Benefits of DLT not clearly evaluated or too much promised because of a lack of knowledge
1. Role of DLT in business case unclear	The benefit and role of DLT can be unclear in the business case, for example the DLT only being used as a replacement of a database.
1. Low understanding of DLT	A lack of understanding about DLT can cause wrong decisions about the technology
2. Vendor ceases to exist	Many players are currently jumping on the hype and there is no guarantee on long-term existence
2. DLT vendor over-promises capabilities	Vendor may over-promise capabilities needed for business but never actually provide these capabilities
2. DLT from vendor not reachable	When the DLT is run off-site at a third party vendor, it might be possible that the connection with the vendor may be lost
3. Critical mass of participants not reached	In order to acchieve benefits from DLT solutions a critical mass of participants must be reached before benefits are realized. For example an entire supply chain.
3. Network participant pulls out	When there is no incentive for participants to stay in the network, it might be possible that they pull out leaving the remaining participants with a potentially incomplete business process.

Table C.1: Risks of Strategic risk area

3. Change management
4. Business continuity

Security

Please note if you would like to include or exclude the listed risks from the strategic high-level risk area. The numbers in front of the risk correspond to the following low level risk areas:

1. Hardware manipulation
2. Software manipulation
3. Identity and access management
4. Disclosure of sensitive information

Legal

Please note if you would like to include or exclude the listed risks from the strategic high-level risk area. The numbers in front of the risk correspond to the following low level risk areas:

1. Regulatory compliance
2. Contractual compliance
3. Legal liability
4. Licensing structure

Development

Please note if you would like to include or exclude the listed risks from the strategic high-level risk area. The numbers in front of the risk correspond to the following low level risk areas:

1. Engineer expertise and skills
2. Integration with existing systems
3. Code complexity
4. Code verification

DLT Platform

Please note if you would like to include or exclude the listed risks from the strategic high-level risk area. The numbers in front of the risk correspond to the following low level risk areas:

1. IoT specific fit
2. Consensus mechanism
3. Data structure
4. Smart contract capability
5. Inter-DLT operability

Parts	Description
1. Slow transactions between nodes	Transactions not processing as quickly as needed by the business process.
1. Slow executing smart contracts	Smart contracts executing slowly because of high traffic
1. Transaction not completed	Because of the non determinism of many DLTs it cannot be guaranteed that a transaction is successfully completed
2. Inaccurate data added to the network	When onboarding data to the network it is possible for it to be inaccurate. Measures should be in place to prevent this.
2. Illegal content added to ledger	It may be possible that participants of the network, intentionally or unintentionally, add illegal content to the ledger.
2. Private data unremovable from ledger	While immutability is one of the key benefits of a DLT, it also poses a great risk with for example private data.
3. No consensus on upgrades of DLT	In order to upgrade a DLT network each participant needs to agree in order to avoid hard forks.
3. Multiple truths	If branching is allowed it is possible to have multiple 'truths' in the network. It needs to be decided which branch to follow.
4. No backup in place for network outage	When business critical processes run on a DLT, a backup should be in place for the event that the DLT does not function properly.
4. Mitigation of risks	A plan should be in place to reduce and mitigate risks of the DLT application
4. No clear governance structure	Clear governance should be in place to reduce the possibility of outages. Close collaboration with change management and data management should be in place.

Table C.2: Risks of Operational risk area

Parts	Description
1. IoT device breached	IoT devices have a high chance of being breached because of their limited security measures. When acting as a node this could potentially gain access to the ledger.
1. IoT device using legacy software	When the IoT device is not up to date, the chances of it being breached increases.
2. Majority of nodes lost	When the majority of nodes is taken over by a malicious party, the integrity of the ledger cannot be guaranteed anymore.
2. Centralization of nodes	With the centralization of nodes the possibility for a malicious attack increases and the chances of a network outage increases.
2. Insecure consensus mechanism	Often times a trade off between performance and security needs to be taken with the chosen consensus mechanism. Low security potentially causes invalid transactions to be approved.
2. Cryptography breached	With advances in cryptography it might be possible that the cryptography of the ledger is breached
2. Data oracle breached	With many DLT implementations there is still a central element feeding data into smart contracts, the oracle. When this oracle is breached, invalid data may be sent to the ledger causing smart contracts to fire when not intended.
3. Identity of participant stolen	Because of a private key infrastructure employed by many blockchains it is possible for a malicious entity to steal the identity of a participant when his or her private key is stolen or lost.
3. No access to network	A participant may lose its private key and therefor potentially its access to the network.
3. Lost or stolen assets	A participant may lose access to its assets because of a lost or stolen private key
4. Business processes revealed	Using data mining on metadata it might be possible to reveal business processes
4. Private data revealed	Private data may be accessed when unsecured on the ledger.

Table C.3: Risks of Security risk area

Parts	Description
1. Not compliant with GDPR legislation	The application may not be compliant with GPDR legislation based on the way private data is managed.
1. Not compliant with KYC and AML legislation	The application may not be compliant with anti money laundering legislation and know your customer banking regulations.
1. Not compliant with future legislation	It might be possible that in the future new legislation is written requiring a change in the application.
2. Not compliant with SLA with customer	The new non-deterministic nature and uncertainty around DLT makes it difficult to predict how well SLAs are handled.
2. Limited SLA with vendor	Many DLT vendors do not not guarantee performance
3. Liable for content that is not your own	It is possible that a participant of the network is liable for content that is not his own.
3. Liable for DAO	When participating in a Decentralized Autonomous Organisation you might be liable for it's malfunction
3. Liable for damages of other participants	When providing a smart contract to other participants, the provider of the contract may be held responsible for malfunction.
4. Software licensing does not allow distribution	Licencing of software may not allow for distribution of the software to other nodes
4. Conflicting licenses	When using multiple software platforms licensing becomes an issue, for example the combination between an Apache 2.0 license and GPL-3.

Table C.4: Risks of Legal risk area

Parts	Description
1. Low DLT programming knowledge	It is hard to find programmers which are knowledgeable on the topic of DLT programming. Be it smart contract programming or setting up the infrastructure.
1. Limited legal knowledge	Programmers which are creating smart contracts may have limited legal knowledge making it difficult to spot legal errors in a legal smart contract
2. DLT and legacy systems not properly integrated	The ledger may not be integrated with legacy systems because of it's complexity
2. Insecure integration with legacy system	Poor integration with legacy systems can cause security issues
3. Code not readable	Because of the complexity of DLT programming the code that is being created may not be well readable
3. Poor documentation	The documentation of DLT may be limited as much code is being developed using rapid prototyping
3. Legacy code creation	Complexity and low knowledge of DLT programming may cause the creation of legacy code not usable in future applications.
4. No testing possible	Because of the non-deterministic nature of many DLT systems it may not be possible to properly test if all the code is working properly
4. New language used	Because of new programming languages used in DLT creation, testing methods may not be available yet.
4. Immutable errors	Due to the immutable nature of DLT it may be possible a code error is immutably set in the ledger

Table C.5: Risks of Development risk area

Parts	Description
1. DLT requires high bandwidth	IoT devices usualy require operation with a limited amount of bandwidth. Some DLT may require high bandwidth to communicate with other nodes and keep consensus.
1. DLT requires high storage	IoT devices usually require operation with a limited amount of storage. Some DLTs may use a lot of storage when copying entire contents of ledger
1. DLT requires high battery usage	IoT devices usually require operation with a limited amount of battery. Some DLTs may use a lot of battery power when computing hashes or communicating with other nodes
1. DLT requires high processing power	IoT devices usually only have small processors. Some DLTs may use a lot of processing power making the IoT device unusable.
2. Consensus mechanism slow	Depending on the consensus mechanism it may be slow and not well fit for IoT devices
2. Consensus mechanism not formally proved	With many new consensus mechanisms proposed, their limitations are often not well documented and their operation not formally proved.
2. Consensus mechanism not secure	The consensus mechanism may prove not to be secure with a large number of malicious participants
3. Poor scalability of network	Depending on the data structure used to save data on the DLT it may cause poor scalability
3. Poor synchronizability	Depending on the data structure used, nodes may have a difficult time staying synchronized with the network
3. Centralization of data	Depending on the data structure used in the DLT, data may become centralized to certain parts of the network.
4. Smart contracts not available	While this may not be an issue for some applications, many require the possibility to run code on the network.

Table C.6: Risks of DLT platform risk area

Additional risks

If you believe that there are any essential risks missing from this list of risks, please add them here. Please bear in mind that this model wil focus on DLT applications with a focus on usage in an IoT based environment.

Comment box to add additional risks.

C.2.3 Final page

Thank you for filling out the survey. If you are interested in how other participants enter the survey you can always check back before the deadline at 27 July at 23:59. It is always possible to change your own answers before the deadline.

The next survey will be sent out on the 9th of August. If in the meantime you have any questions or comments, please let me know at j.vermeij-1@student.utwente.nl or fixed-term.jaap.vermeij@de.bosch.com.

Appendix D

Final Model Elements

D.1 Criteria for usage

- IoT devices should be used within the DLT application or allow for the possibility to use them.
- DLT application is benefitted by higher transaction speeds.
- DLT application is created by a business and used for B2B or B2C interactions.

D.2 Level Descriptions and Assessment statements

D.2.1 Overall Maturity Level Descriptions

Level 1. Ad hoc - No processes to handle the identified risks. Risks are not consistently addressed only and on an informal basis.

Level 2. Initial - Processes are in place to handle risks but they are not standardized. Often times risks are mitigated after the risk has taken place.

Level 3. Repeatable - Processes are characterized to handle identified risks and are standardized. Processes are proactive in identifying and mitigating the risks.

Level 4. Managed - Processes in place to control the identified risks based on continuous measurement and control

Level 5. Optimizing - Continuously looking for possibilities to improve processes of mitigating the identified risks.

D.2.2 DLT Platform Choice

Level Descriptions

Level 1. Platform is chosen based on availability of technology or developmental experience of developers. There has been a basic analysis for fit for the use case based on experience of developers.

Level 2. Requirement analysis for the use case has been performed to analyze the fit for the use case.

Level 3. Pre-defined criteria are in place to measure fit of a platform to a use case.

Level 4. Processes in place for optimization of platform based on changing needs of the use case.

Level 5. Recurring comparative analysis is in place to evaluate and optimize the platform throughout it's lifetime.

Assessment Statements

Level	Statement	Required
1	The platform has been chosen based on the experience of the developers.	0
1	The platform has been chosen based on what is available.	0
2	A requirement analysis for the use case has been performed to analyze what type of platform is needed.	1
3	The criteria for fit of a DLT platform to a use case have been standardized.	1
4	The platform needs for the use case are periodically examined.	1
4	Processes in place to optimize existing platform or switch platform if needed	1
5	The platform is continuously evaluated through pre-defined criteria	1
5	The platform is periodically compared to other platforms to evaluate the best fit	1

D.2.3 DLT Ecosystem Partners

Level Descriptions

Level 1. The application is only run internally in a closed environment without partners.

Level 2. The application is run within a consortium of businesses with each participant performing a single unique function in the network. When one participant decides to stop using the system the network will lose functionality.

Level 3. The application is run within a consortium of businesses with multiple participants performing similar functions within the network. Agreements are in place with ecosystems partners to ensure a consensus driven improvement process of the network.

Level 4. When one participant decides to stop using the system only the related process with that single participant are effected without overall the network losing functionality. Partners are actively recruited by an active governance structure of the network.

Level 5. Each participant is actively managing and improving the network. New partners are actively asking to join network due to market leadership.

Assessment Statements

Level	Statement	Required
1	The network behind the DLT application is run internally without external partners	0
2	The application runs on a network with external partners	1
2	Each participant performs a single unique function in network	0
2	The network loses critical functionality when one participant leaves the network	0
3	The network contains participants who perform similar functions	1
3	Improvements for the application are handled through a consensus driven improvement process	0
3	Agreements in place to ensure participants stay in network	0
4	When a participant leaves the network only the related process with that participant are effected, not the whole network	1
4	An active governance of the network aims to recruit new partners	0
5	The majority of network is involved in improving the network	1
5	New participants are actively joining due to market leadership	1

D.2.4 DLT Application Performance

Level 1. Simple usability tests are performed on the application and a small scale qualitative performance tests are performed.

Level 2. Performance of application has been tested once quantitatively using key metrics with production-like circumstances.

Level 3. Periodic testing of performance using predefined key metrics and processes are in place to request extra resources in order to increase performance.

Level 4. Continuous measurement of application performance using predefined key metrics with notification when performance falls under specified minimum.

Level 5. Continuously optimizing DLT application performance. Continuously optimizing resources to achieve optimum level of performance.

Assessment Statements

Level	Statement	Required
1	Usability tests have been performed to test functionality of application	0
1	(Small-scale) qualitative performance tests have been performed	1
2	Quantitative testing has been performed with production-like circumstances	1
2	Key metrics have been defined to test performance of DLT application	1
3	Minimum and target performance specified using predefined metrics	1
3	Performance testing is done periodically	0
3	Processes in place to request extra resources in case of poor performance	1
4	The performance of the DLT application is continuously measured	1
4	Relevant stakeholder is automatically notified when performance drops under specified minimum	1
5	Resources are continuously optimized to reach target performance	1

D.2.5 Data Management

Level 1. Data that is in the ledger is assumed to be accurate and no procedures are in place to verify accuracy. All data is able to be added to the ledger.

Level 2. After an incident relating to inaccurate data on the chain takes place, the accuracy of data is checked according to procedures which are previously defined and documented for data inspection. Procedures are in place to identify illegal data on the ledger.

Level 3. Data validation checks are in place for all data providers to ensure data accuracy. Accuracy of provided data is auditable by other participants. Illegal data are being automatically barred by a front-end from being onboarded onto the ledger.

Level 4. A monitoring system is in place to automatically verify data accuracy, when data cannot prove it's accuracy it is not allowed on the ledger from the network side.

Level 5. All added data on the ledger is accurate and auditable. Procedures to remove or block private or illegal data are in place without losing the integrity of data on the ledger.

Assessment Statements

Level	Statement	Required
1	Assumptions are made about the accuracy of data on the ledger	0
1	There are no procedures to verify accuracy of data	0
1	All data can be added to the ledger	0
2	After an incident caused by inaccurate data, accuracy of data is checked according to previously defined procedures	1
3	Data validation checks are in place for all network participants	0
3	Accuracy of data is auditable by other participants	1
3	Data identified as illegal is blocked from the ledger by a front end	0
4	A network monitoring system automatically verifies data accuracy and blocks inaccurate data	1
5	Procedures are in place to remove or block data identified as illegal without losing integrity of the ledger	1

D.2.6 Change Management

Level 1. Changes to application running on DLT are made ad-hoc by central authority with little collaboration with ecosystem partners.

Level 2. Process in place for ecosystem partners to challenge changes proposed by central authority.

Level 3. Governance structure in place to handle changes to the application with one central authority but the possibility for ecosystem partners to suggest changes.

Level 4. Governance structure in place with small consortium who decide on changes to the application.

Level 5. Open governance structure with all entities able to contribute code and balanced voting power distributed over all participants.

Assessment Statements

Level	Statement	Required
1	Changes are applied ad-hoc by a central authority	0
2	Changes are proposed by central authority	0
2	Ecosystem partners can challenge proposals	1
3	Governance structure with one central authority is in place to handle changes	0
3	Each participant can propose changes	1
4	Consortium governance structure handles changes to the application	0
5	Open governance structure to handle changes with balanced voting distributed over all participants	1

D.2.7 Endpoint Security

Level 1. Reliance on inherent DLT characteristics to protect network from malicious nodes in the network.

Level 2. Requirements for devices are distributed to providers of IoT devices that participate in network which cover main use cases and well-known security incidents in similar environments.

Level 3. Permissioned network with extended security requirements for devices which are based on best practice, standards, regulations and classifications, is in place. Devices are checked to identify if they comply with the required security characteristics before they are allowed to join the network.

Level 4. Network with automatic access restrictions when joining based on dynamic adaptable security framework tendered to resource limitations of device.

Level 5. Measures are in place to detect and restrict access to malicious devices based on usage patterns of the device.

Assessment Statements

Level	Statement	Required
1	All nodes are accepted to join the network	0
2	Basic security requirements for IoT devices distributed to network participants as guidelines	0
3	Extensive security requirements based on best practice, standards, regulations and classification in place for IoT devices.	1
3	Only devices which pass security requirements are accepted to join the network	0
4	Dynamically adaptable security framework in place	1
4	Network based access restrictions based on adaptable security framework	1
5	Automatic anomaly detection of potential malicious devices based on usage patterns of the device	1
5	Automatic network access restriction based on anomaly detection	1

D.2.8 DLT Protocol Attacks

Level 1. Episodic risk assessment performed based on minimal understanding of related DLT protocol risks. No processes in place to mitigate risks.

Level 2. Analysis performed based on select known security risks. Worst-case scenarios are focus. Periodic assessment of risks and mitigation strategies defined.

Level 3. Extensive analysis on possible security risks performed. Amount of accepted risks defined. Mitigation strategies in place to reach the accepted risks.

Level 4. Automatic detection of risks based on defined DLT protocol risks. Mitigation strategies defined or adapted when risk is identified.

Level 5. Automatic detection of security risks and improvement of detection based on learning algorithm. Mitigation automatically adapted to reach desired acceptance of risks.

Assessment Statements

Level	Statement	Required
1	Episodic risk assessment based on basic understanding of DLT protocol risks	0
1	No processes to mitigate risks if they occur	0
2	Risk analysis based on known DLT security risks from practice	0
2	Focus of risk analysis is on worst-case scenarios	0
2	Periodic assessment of risks and mitigation strategies in place	0
3	Extensive risk assessment in place to identify possible security risks	1
3	Accepted and desired risk levels are defined	1
3	Mitigation strategies in place to reach acceptable risk level.	1
4	Risks are detected automatically based on defined DLT protocol risks	1
4	Mitigation strategies are defined and adapted when risk is identified	0
5	Risks are detected automatically through a learning algorithm	1
5	Mitigation strategies automatically adapted to reach desired level of risk	1

D.2.9 Identity Management

Level 1. Single points of failure in key storage evident. Keys are created ad-hoc and not stored in a consistent method.

Level 2. Key management system is available to store keys and give access to individuals. Policies defined to create and gain access to keys defined per project.

Level 3. Policies in place to proactively reduce risks of stolen and lost keys with methods like key rotation. Storage and creation of keys through hardware security modules.

Level 4. Monitoring anomalies in network and key management system in order to identify possible instances of malicious use of keys. Processes in place to revoke keys.

Level 5. Continuous improvement of identity management investigating alternative identity systems and improving current key management systems.

Assessment Statements

Level	Statement	Required
1	Keys are stored at a single point	0
1	Keys are created ad-hoc when they are needed	0
1	Keys are not stored in a consistent matter	0
2	Key management system is in place to give access to individuals	1
2	Policies defined to create keys within a project	1
2	Policies defined to gain access to keys within a project	1
3	There are policies in place to proactively reduce risks of stolen and lost keys	1
3	Storage and creation of keys handled through hardware security modules	1
4	Anomalies in the network are monitored for malicious use of keys	1
4	Anomalies in the key management system are monitored for malicious use of keys	1
4	There are processes in place to revoke keys	1
5	Identity management system is continuously improved	1
5	Alternative identity systems are investigated	1
5	Current key management systems are continuously improved	1

D.2.10 Transactional Security

Level 1. Transactions are open for other participants in the network to view and no processes are in place to ensure no sensitive data is added to the ledger.

Level 2. Per transaction there is a manual process to ensure no sensitive data is added to the chain. Sensitive data is not clearly defined.

Level 3. There is an automatic process to ensure no sensitive data is added to the ledger. There is a clear definition for data which may and may not be added to the ledger.

Level 4. Measures are taken in order to reduce the possibility of information to be gathered from the contents or metadata of transactions.

Level 5. Continuous improvement of transactional security mechanisms including auditing testing of mechanisms to ensure security.

Assessment Statements

Level	Statement	Required
1	Contents of transactions are open for other participants in the network to view	0
1	No processes to reduce the amount of sensitive data on the ledger	0
2	Manual process per transaction is in place to ensure no sensitive data is added to the chain	0
2	Sensitive data is defined at the discretion of the user	0
3	An automatic process is in place for all transactions to ensure no sensitive data is added to the ledger	0
3	Sensitive data is clearly defined on a company wide basis	1
4	There are measures in place to reduce the possibility of information to be gathered from the contents of transactions	1
4	There are measures in place to reduce the possibility of information to be gathered from the metadata of transactions	1
5	Transactional security mechanisms are continuously improved using methods like external audit testing	1

D.2.11 Regulatory Compliance

Level 1. No formal evaluation of compliance with legislation is performed. Evaluations that are performed are inconsistently applied, informal and incomplete.

Level 2. Evaluation of compliance is performed after development of the application. There are some compliance controls in place but they are not integrated into the overall compliance management of the organization.

Level 3. Compliance with regulation is taken into account during the development of the application. Compliance controls integrated and standardized across the organization.

Level 4. Legislative outlook is performed to evaluate compliance with possible future regulations. Periodic reviews are conducted to assess the effectiveness and completeness of the compliance controls.

Level 5. Regular review and feedback are used to ensure continuous improvement towards optimization of compliance processes.

Assessment Statements

Level	Statement	Required
1	No formal evaluation of legislation compliance has taken place	0
1	Evaluations that are performed are inconsistently applied, informal and incomplete	0
2	After development of application a formal evaluation of compliance has been performed	1
2	Some compliance controls are in place but they are not integrated with the rest of the organization	0
3	Compliance with regulation is taken into account during the development of the application	1
3	Compliance controls are integrated and standardized across the organization	1
4	Legislative outlook has been performed to evaluate compliance with future legislation	1
4	Periodic reviews are conducted to assess effectiveness and completeness of compliance controls	1
5	Regular review and feedback between all involved parties are in place to ensure continuous improvement of the compliance process	1

D.2.12 Legal Liability

Level 1. No formal evaluation of possible liability risks performed. Evaluations that are performed are inconsistently applied, informal and incomplete.

Level 2. Evaluation of liability performed after development of the application. Liability evaluated based on agreements with ecosystem partners. Liability risks are partly mitigated through contractual agreements between participants. No further evaluation of tort or partnership liability risks.

Level 3. Liability risks are taken into account during development of the application. Evaluation during development based on legal knowledge of the developers. All legal risks are evaluated by a specialized legal department before deployment of the application.

Level 4. Liability risks are constantly monitored by legal department and direct feedback is given to developers responsible for the application.

Level 5. Monitoring of legislation and case law by legal department is carried out to identify possible DLT liability risks. Development of application performed with possible future legislation in mind.

Assessment Statements

Level	Statement	Required
1	No formal evaluation of liability risks has taken place	0
1	Evaluations that are performed are inconsistently applied, informal and incomplete	0
2	After development of application a formal evaluation of liability has been performed	1
2	Liability is evaluated based on agreements with ecosystem partners	0
2	Liability risks are mitigated through contractual agreements between parties	0
3	Liability risks are taken into account during development of the application	1
3	Evaluation during development based on legal knowledge of developers	0
3	All legal risks evaluated by legal department before deployement of application	0
4	Liability risks are continuously monitored by legal department with direct feedback to developers	1
5	Legislation is monitored to identify possible future DLT liability risks	1
5	Application is developed with future legislation in mind	1

D.2.13 Integration with Existing Systems

Level 1. The DLT application runs separately from all other existing applications. Manual input needed to transfer information from existing systems.

Level 2. Different connections between DLT application and existing applications are separately developed. Connections with existing applications are evaluated for known security weaknesses. Assessment has been performed to test the functionality of the integration.

Level 3. Single secure interface or standard for interface exists for existing applications to interact with DLT application.

Level 4. Interface with existing applications are being continuously monitored for errors and security incident detection features exist.

Level 5. Continuous monitoring for improvements to the interfaces and reducing complexity of interfaces where possible. Adaptive integration infrastructure that can handle changes when DLT standards evolve.

Assessment Statements

Level	Statement	Required
1	DLT runs separately from all other applications within the company	0
1	Manual input is needed to transfer information from existing systems	0
2	Different connections between DLT application and existing systems are in place and separately developed	0
2	Connections with existing systems are evaluated for known security weaknesses	1
2	Assessment has been performed to test functionality of the connection	1
3	Single secure interface is in place for existing applications to interact with the DLT application	0
4	Interface with existing applications are monitored for errors	1
4	Security incident detection features exist for the interfaces with existing systems	1
5	Continuous monitoring of interfaces for improvements	1
5	Complexity of interfaces is reduced where possible	1
5	Integration infrastructure is adaptable to changes when DLT evolves	1

D.2.14 Code Quality

Level 1. Knowledge on code is silo-ed, includes many home-grown solutions and unmodifiable legacy code. Code is buggy but functions if you know how to avoid the buggy areas. Lack of skilled engineers available to create application.

Level 2. Code works and matches the requirements of the application. Code includes duplicate solutions to same problems. Code is difficult to understand by another software engineer.

Level 3. Code is well documented and modern design patterns are used to create code. Code is readable by another software engineer. Skilled software engineers available to create the application.

Level 4. Code is modular, reusable and easily accessible to other DLT applications. Software engineers with experience in DLT development available to develop applications.

Level 5. Quality of code can be quantitatively measured and the development is being continuously improved.

Assessment Statements

Level	Statement	Required
1	Knowledge of the codebase of the application is silo-ed	0
1	Codebase includes home-grown solutions	0
1	Unmodifiable legacy code exists because no one knows how it works anymore	0
1	Code is buggy but functions	0
1	Skilled engineers are not available to create application	0
2	Code works and matches requirements of the application	1
2	Code has duplicate solutions to the same problems	0
2	Code may be difficult to understand by another software engineer	0
3	Code is well documented	1
3	Modern design patters are used to create code	1
3	Code is readable by other software engineer	1
3	Skilled engineers are available to create the application	1
4	Code is modular and reusable by other DLT applications	1
4	Software engineers with experience in DLT development available	1
5	Quality of code can be quantitatively measured	1

D.2.15 Code Verification

Level 1. Code is proprietary and has not been formally proven.

Level 2. Code is audited based on functional testing.

Level 3. Code is audited based on functional and non-functional testing and external auditing by programs such as open sourcing or bug bounty programs.

Level 4. Test-driven development with continuous testing throughout development. Using techniques such as model driven engineering to allow for non-developers to check code.

Level 5. Continuous improvement of code verification with additional programs to further test the code when released.

Assessment Statements

Level	Statement	Required
1	Code is proprietary and has not been formally proven	0
2	Code is audited based on functional testing	0
3	Code is audited based on functional and non-functional testing	1
3	External auditing programs are in place	1
4	Development is through test-driven development principles	1
4	Non-developers are able to check code with methods like model-driven engineering	1
5	Code verification procedures continuously improved with additional programs to test code when released	1

Appendix E

Back-end Dashboard Files

E.1 SQL Script

The following script can be used to create and populate the database used as a back end of the IT Risk Maturity Model Dashboard for DLT Applications. The script works for MySQL 8.0 databases but can also be applied to other databases.

E.1.1 Schema creation

```
CREATE SCHEMA IF NOT EXISTS `dlt_maturity_model` DEFAULT CHARACTER SET utf8 ;
USE `dlt_maturity_model` ;

-- -----------------------------------------------------
-- Table `dlt_maturity_model`.`riskAreas`
-- -----------------------------------------------------
CREATE TABLE IF NOT EXISTS `dlt_maturity_model`.`riskAreas` (
  `id` INT UNSIGNED NOT NULL AUTO_INCREMENT,
  `name` VARCHAR(45) NULL,
  `description` VARCHAR(255) NULL,
  PRIMARY KEY (`id`))
ENGINE = InnoDB;


-- -----------------------------------------------------
-- Table `dlt_maturity_model`.`subRiskAreas`
-- -----------------------------------------------------
CREATE TABLE IF NOT EXISTS `dlt_maturity_model`.`subRiskAreas` (
  `id` INT UNSIGNED NOT NULL AUTO_INCREMENT,
  `name` VARCHAR(45) NULL,
  `description` MEDIUMTEXT NULL,
  `riskAreas_id` INT UNSIGNED NOT NULL,
  PRIMARY KEY (`id`),
  INDEX `fk_subRiskAreas_riskAreas_idx` (`riskAreas_id` ASC) VISIBLE,
  CONSTRAINT `fk_subRiskAreas_riskAreas`
    FOREIGN KEY (`riskAreas_id`)
```

```
    REFERENCES `dlt_maturity_model`.`riskAreas` (`id`)
    ON DELETE NO ACTION
    ON UPDATE NO ACTION)
ENGINE = InnoDB;


-- -----------------------------------------------------
-- Table `dlt_maturity_model`.`mainMaturityLevels`
-- -----------------------------------------------------
CREATE TABLE IF NOT EXISTS `dlt_maturity_model`.`mainMaturityLevels` (
  `id` INT UNSIGNED NOT NULL AUTO_INCREMENT,
  `level` INT NULL,
  `description` MEDIUMTEXT NULL,
  PRIMARY KEY (`id`))
ENGINE = InnoDB;


-- -----------------------------------------------------
-- Table `dlt_maturity_model`.`subMaturityLevels`
-- -----------------------------------------------------
CREATE TABLE IF NOT EXISTS `dlt_maturity_model`.`subMaturityLevels` (
  `id` INT UNSIGNED NOT NULL AUTO_INCREMENT,
  `description` MEDIUMTEXT NULL,
  `subRiskAreas_id` INT UNSIGNED NOT NULL,
  `mainMaturityLevels_id` INT UNSIGNED NOT NULL,
  PRIMARY KEY (`id`),
  INDEX `fk_subMaturityLevels_subRiskAreas1_idx` (`subRiskAreas_id` ASC) VISIBLE,
  INDEX `fk_subMaturityLevels_mainMaturityLevels1_idx` (`mainMaturityLevels_id` ASC)
  ↪ VISIBLE,
  CONSTRAINT `fk_subMaturityLevels_subRiskAreas1`
    FOREIGN KEY (`subRiskAreas_id`)
    REFERENCES `dlt_maturity_model`.`subRiskAreas` (`id`)
    ON DELETE NO ACTION
    ON UPDATE NO ACTION,
  CONSTRAINT `fk_subMaturityLevels_mainMaturityLevels1`
    FOREIGN KEY (`mainMaturityLevels_id`)
    REFERENCES `dlt_maturity_model`.`mainMaturityLevels` (`id`)
    ON DELETE NO ACTION
    ON UPDATE NO ACTION)
ENGINE = InnoDB;


-- -----------------------------------------------------
-- Table `dlt_maturity_model`.`statements`
-- -----------------------------------------------------
CREATE TABLE IF NOT EXISTS `dlt_maturity_model`.`statements` (
  `id` INT UNSIGNED NOT NULL AUTO_INCREMENT,
```

```
  `subMaturityLevels_id` INT UNSIGNED NOT NULL,
  `description` MEDIUMTEXT NULL,
  `required` TINYINT NULL,
  PRIMARY KEY (`id`),
  INDEX `fk_statements_subMaturityLevels1_idx` (`subMaturityLevels_id` ASC) VISIBLE,
  CONSTRAINT `fk_statements_subMaturityLevels1`
    FOREIGN KEY (`subMaturityLevels_id`)
    REFERENCES `dlt_maturity_model`.`subMaturityLevels` (`id`)
    ON DELETE NO ACTION
    ON UPDATE NO ACTION)
ENGINE = InnoDB;
```

E.1.2 Data population

```
INSERT INTO riskAreas(id,name,description) VALUES (1,'Strategic','Risks arising from
↪  strategic decisions surrounding the choice for a DLT and the partners in the
↪  network.');
INSERT INTO riskAreas(id,name,description) VALUES (2,'Operational','Risks arising
↪  from inadequate or failed processes, people or systems surrounding the DLT
↪  application.');
INSERT INTO riskAreas(id,name,description) VALUES (3,'Security','Risks arising from
↪  security incidents surrounding the DLT and IoT devices.');
INSERT INTO riskAreas(id,name,description) VALUES (4,'Legal','Risks arising from
↪  legal challenges surrounding the DLT application.');
INSERT INTO riskAreas(id,name,description) VALUES (5,'Development','Risks arising
↪  during and around the development of the DLT application.');

INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (1,'DLT platform
↪  choice',NULL,1);
INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (2,'DLT ecosystem
↪  partners',NULL,1);
INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (3,'DLT
↪  application performance',NULL,2);
INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (4,'Data
↪  management',NULL,2);
INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (5,'Change
↪  management',NULL,2);
INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (6,'Endpoint
↪  security',NULL,3);
INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (7,'DLT protocol
↪  attacks',NULL,3);
INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (8,'Identity
↪  management',NULL,3);
INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (9,'Transaction
↪  security',NULL,3);
INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (10,'Regulatory
↪  compliance',NULL,4);
```

```
INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (11,'Legal
↪  liability',NULL,4);
INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (12,'Integration
↪  with existing systems',NULL,5);
INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (13,'Code
↪  quality',NULL,5);
INSERT INTO subRiskAreas(id,name,description,riskAreas_id) VALUES (14,'Code
↪  verification',NULL,5);

INSERT INTO mainMaturityLevels(id,level,description) VALUES (1,1,'Ad hoc - No
↪  processes to handle the identified risks. Risks are not consistently addressed
↪  only and on an informal basis.');
INSERT INTO mainMaturityLevels(id,level,description) VALUES (2,2,'Initial -
↪  Processes are in place to handle risks but they are not standardized. Often
↪  times risks are mitigated after the risk has taken place.');
INSERT INTO mainMaturityLevels(id,level,description) VALUES (3,3,'Repeatable -
↪  Processes are characterized to handle identified risks and are standardized.
↪  Processes are proactive in identifying and mitigating the risks.');
INSERT INTO mainMaturityLevels(id,level,description) VALUES (4,4,'Managed -
↪  Processes in place to control the identified risks based on continuous
↪  measurement and control');
INSERT INTO mainMaturityLevels(id,level,description) VALUES (5,5,'Optimizing -
↪  Continuously looking for possibilities to improve processes of mitigating the
↪  identified risks.');

INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (1,'Platform is chosen based on availability of technology or
↪  developmental experience of developers. There has been a basic analysis for fit
↪  for the use case based on experience of developers.',1,1);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (2,'Requirement analysis for the use case has been performed to analyze
↪  the fit for the use case.',1,2);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (3,'Pre-defined criteria are in place to measure fit of a platform to a
↪  use case.',1,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (4,'Processes in place for optimization of platform based on changing
↪  needs of the use case.',1,4);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (5,'Recurring comparative analysis is in place to evaluate and optimize
↪  the platform throughout it''s lifetime.',1,5);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (6,'The application is only run internally in a closed environment
↪  without partners.',2,1);
```

```
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (7,'The application is run within a consortium of businesses with each
↪ participant performing a single unique function in the network. When one
↪ participant decides to stop using the system the network will lose
↪ functionality.',2,2);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (8,'The application is run within a consortium of businesses with
↪ multiple participants performing similar functions within the network.
↪ Agreements are in place with ecosystems partners to ensure a consensus driven
↪ improvement process of the network.',2,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (9,'When one participant decides to stop using the system only the
↪ related process with that single participant are effected without overall the
↪ network losing functionality. Partners are actively recruited by an active
↪ governance structure of the network.',2,4);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (10,'Each participant is actively managing and improving the network. New
↪ partners are actively asking to join network due to market leadership.',2,5);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (11,'Simple usability tests are performed on the application and a small
↪ scale qualitative performance tests are performed.',3,1);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (12,'Performance of application has been tested once quantitatively using
↪ key metrics with production-like circumstances.',3,2);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (13,'Periodic testing of performance using predefined key metrics and
↪ processes are in place to request extra resources in order to increase
↪ performance.',3,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (14,'Continuous measurement of application performance using predefined
↪ key metrics with notification when performance falls under specified
↪ minimum.',3,4);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (15,'Continuously optimizing DLT application performance. Continuously
↪ optimizing resources to acchieve optimum level of performance.',3,5);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (16,'Data that is in the ledger is assumed to be accurate and no
↪ procedures are in place to verify accuracy. All data is able to be added to the
↪ ledger.',4,1);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (17,'After an incident relating to inaccurate data on the chain takes
↪ place, the accuracy of data is checked according to procedures which are
↪ previously defined and documented for data inspection. Procedures are in place
↪ to identify illegal data on the ledger.',4,2);
```

```
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (18,'Data validation checks are in place for all data providers to ensure
↪ data accuracy. Accuracy of provided data is auditable by other participants.
↪ Illegal data are being automatically barred by a front-end from being onboarded
↪ onto the ledger.',4,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (19,'A monitoring system is in place to automatically verify data
↪ accuracy, when data cannot prove it''s accuracy it is not allowed on the ledger
↪ from the network side.',4,4);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (20,'All added data on the ledger is accurate and auditable. Procedures
↪ to remove or block illegal data are in place without losing the integrity of
↪ data on the ledger.',4,5);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (21,'Changes to application running on DLT are made ad-hoc by central
↪ authority with little collaboration with ecosystem partners.',5,1);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (22,'Process in place for ecosystem partners to challenge changes
↪ proposed by central authority.',5,2);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (23,'Governance structure in place to handle changes to the application
↪ with one central authority but the possibility for ecosystem partners to suggest
↪ changes.',5,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (24,'Governance structure in place with consortium who handle changes to
↪ the application.',5,4);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (25,'Open governance structure with all entities able to contribute code
↪ and balanced voting power distributed over all participants.',5,5);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (26,'Reliance on inherent DLT characteristics to protect network from
↪ malicious nodes in the network.',6,1);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (27,'Requirements for devices are distributed to providers of IoT devices
↪ that participate in network which cover main use cases and well-known security
↪ incidents in similar environments.',6,2);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (28,'Permissioned network with extended security requirements for devices
↪ which are based on best practice, standards, regulations and classifications, is
↪ in place. Devices are checked to identify if they comply with the required
↪ security characteristics before they are allowed to join the network.',6,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (29,'Network with automatic access restrictions when joining based on
↪ dynamic adaptable security framework tendered to resource limitations of
↪ device.',6,4);
```

```
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (30,'Measures are in place to detect and restrict access to malicious
↪  devices based on usage patterns of the device.',6,5);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (31,'Episodic risk assessment performed based on minimal understanding of
↪  related DLT protocol risks. No processes in place to mitigate risks.',7,1);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (32,'Analysis performed based on select known security risks. Worst-case
↪  scenarios are focus. Periodic assessment of risks and mitigation strategies
↪  defined.',7,2);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (33,'Extensive analysis on possible security risks performed. Amount of
↪  accepted risks defined. Mitigation strategies in place to reach the accepted
↪  risks.',7,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (34,'Automatic detection of risks based on defined DLT protocol risks.
↪  Mitigation strategies defined or adapted when risk is identified.',7,4);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (35,'Automatic detection of security risks and improvement of detection
↪  based on learning algorithm. Mitigation automatically adapted to reach desired
↪  acceptance of risks.',7,5);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (36,'Single points of failure in key storage evident. Keys are created
↪  ad-hoc and not stored in a consistent method.',8,1);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (37,'Key management system is available to store keys and give access to
↪  individuals. Policies defined to create and gain access to keys defined per
↪  project.',8,2);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (38,'Policies in place to proactively reduce risks of stolen and lost
↪  keys with methods like key rotation. Storage and creation of keys through
↪  hardware security modules.',8,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (39,'Monitoring anomalies in network and key management system in order
↪  to identify possible instances of malicious use of keys. Processes in place to
↪  revoke keys.',8,4);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (40,'Continuous improvement of identity management investigating
↪  alternative identity systems and improving current key management
↪  systems.',8,5);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (41,'Transactions are open for other participants in the network to view
↪  and no processes are in place to ensure no sensitive data is added to the
↪  ledger.',9,1);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (42,'Per transaction there is a manual process to ensure no sensitive
↪  data is added to the chain. Sensitive data is not clearly defined.',9,2);
```

```
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (43,'There is an automatic process to ensure no sensitive data is added
↪ to the ledger. There is a clear definition for data which may and may not be
↪ added to the ledger.',9,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (44,'Measures are taken in order to reduce the possibility of information
↪ to be gathered from the contents or metadata of transactions.',9,4);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (45,'Continuous improvement of transactional security mechanisms
↪ including auditing testing of mechanisms to ensure security.',9,5);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (46,'No formal evaluation of compliance with legislation is performed.
↪ Evaluations that are performed are inconsistently applied, informal and
↪ incomplete.',10,1);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (47,'Evaluation of compliance is performed after development of the
↪ application. There are some compliance controls in place but they are not
↪ integrated into the overall compliance management of the organization.',10,2);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (48,'Compliance with regulation is taken into account during the
↪ development of the application. Compliance controls integrated and standardized
↪ across the organization.',10,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (49,'Legislative outlook is performed to evaluate compliance with
↪ possible future regulations. Periodic reviews are conducted to assess the
↪ effectiveness and completeness of the compliance controls.',10,4);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (50,'Regular review and feedback are used to ensure continuous
↪ improvement towards optimization of compliance processes.',10,5);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (51,'No formal evaluation of possible liability risks performed.
↪ Evaluations that are performed are inconsistently applied, informal and
↪ incomplete.',11,1);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (52,'Evaluation of liability performed after development of the
↪ application. Liability evaluated based on agreements with ecosystem partners.
↪ Liability risks are partly mitigated through contractual agreements between
↪ participants. No further evaluation of tort or partnership liability
↪ risks.',11,2);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (53,'Liability risks are taken into account during development of the
↪ application. Evaluation during development based on legal knowledge of the
↪ developers. All legal risks are evaluated by a specialized legal department
↪ before deployment of the application.',11,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪ VALUES (54,'Liability risks are constantly monitored by legal department and
↪ direct feedback is given to developers responsible for the application.',11,4);
```

```
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (55,'Monitoring of legislation and case law by legal department is
↪  carried out to identify possible DLT liability risks. Development of application
↪  performed with possible future legislation in mind.',11,5);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (56,'The DLT application runs separately from all other existing
↪  applications. Manual input needed to transfer information from existing
↪  systems',12,1);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (57,'Different connections between DLT application and existing
↪  applications are separately developed. Connections with existing applications
↪  are evaluated for known security weaknesses. Assessment has been performed to
↪  test the functionality of the integration.',12,2);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (58,'Single secure interface or standard for interface exists for
↪  existing applications to interact with DLT application.',12,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (59,'Interface with existing applications are being continuously
↪  monitored for errors and security incident detection features exist.',12,4);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (60,'Continuous monitoring for improvements to the interfaces and
↪  reducing complexity of interfaces where possible. Adaptive integration
↪  infrastructure that can handle changes when DLT standards evolve.',12,5);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (61,'Knowledge on code is silo-ed, includes many home-grown solutions and
↪  unmodifiable legacy code. Code is buggy but functions if you know how to avoid
↪  the buggy areas. Lack of skilled engineers available to create
↪  application.',13,1);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (62,'Code works and matches the requirements of the application. Code
↪  includes duplicate solutions to same problems. Code is difficult to understand
↪  by another software engineer.',13,2);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (63,'Code is well documented and modern design patterns are used to
↪  create code. Code is readable by another software engineer. Skilled software
↪  engineers available to create the application.',13,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (64,'Code is modular, reusable and easily accessible to other DLT
↪  applications. Software engineers with experience in DLT development available to
↪  develop applications.',13,4);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (65,'Quality of code can be quantitatively measured and the development
↪  is being continuously improved.',13,5);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (66,'Code is proprietary and has not been formally proven.',14,1);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (67,'Code is audited based on functional testing.',14,2);
```

```
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (68,'Code is audited based on functional and non-functional testing and
↪  external auditing by programs such as open sourcing or bug bounty
↪  programs.',14,3);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (69,'Test-driven development with continuous testing throughout
↪  development. Using techniques such as model driven engineering to allow for
↪  non-developers to check code.',14,4);
INSERT INTO subMaturityLevels(id,description,subRiskAreas_id,mainMaturityLevels_id)
↪  VALUES (70,'Continuous improvement of code verification with additional programs
↪  to further test the code when released.',14,5);


INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (1,1,'The platform has been chosen based on the experience of the
↪  developers.',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (2,1,'The platform has been chosen based on what is available.',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES (3,2,'A
↪  requirement analysis for the use case has been performed to analyze what type of
↪  platform is needed.',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (4,3,'The criteria for fit of a DLT platform to a use case have been
↪  standardized.',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (5,4,'The platform needs for the use case are periodically examined.',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (6,4,'Processes in place to optimize existing platform or switch platform if
↪  needed',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (7,5,'The platform is continuously evaluated through pre-defined criteria',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (8,5,'The platform is periodically complared to other platforms to evaluate the
↪  best fit',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (9,6,'The network behind the DLT application is run internally without external
↪  partners',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (10,7,'The application runs on a network with external partners',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (11,7,'Each participant performs a single unique function in network',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (12,7,'The network loses critical functionality when one participant leaves the
↪  network',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (13,8,'The network contains participants who perform similar functions',1);
```

```
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (14,8,'Improvements for the application are handled through a consesnsus driven
↪  improvement process',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (15,8,'Agreements in place to ensure participants stay in network',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (16,9,'When a participant leaves the network only the related process with that
↪  participant are effected, not the whole network',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (17,9,'An active governance of the network aims to recruit new partners',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (18,10,'The majority of network is involved in improving the network',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (19,10,'New participants are actively joining due to market leadership',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (20,11,'Usability tests have been performed to test functionality of
↪  application',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (21,11,'(Small-scale) qualitative performance tests have been performed',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (22,12,'Quantitative testing has been performed with production-like
↪  circumstances',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (23,12,'Key metrics have been defined to test performance of DLT
↪  application',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (24,13,'Minimum and target performance specified using predefined metrics',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (25,13,'Performance testing is done periodically',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (26,13,'Processes in place to request extra resources in case of poor
↪  performance',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (27,14,'The performance of the DLT application is continuously measured',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (28,14,'Relevant stakeholder is automatically notified when performance drops
↪  under specified minimum',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (29,15,'Resources are continuously optimized to reach target performance',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (30,16,'Assumptions are made about the accuracy of data on the ledger',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (31,16,'There are no procedures to verify accuracy of data',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (32,16,'All data can be added to the ledger',0);
```

```
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (33,17,'After an incident caused by inaccurate data, accuracy of data is checked
↪  according to previously defined procedures',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (34,18,'Data validation checks are in place for all network participants',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (35,18,'Accuracy of data is auditable by other participants',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (36,18,'Data identified as illegal is blocked from the ledger by a front
↪  end',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (37,19,'A network monitoring system automatically verifies data accuracy and
↪  blocks inaccurate data',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (38,20,'Procedures are in place to remove or block data identified as illegal
↪  without losing integrity of the ledger',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (39,21,'Changes are applied ad-hoc by a central authority',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (40,22,'Changes are proposed by central authority',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (41,22,'Ecosystem partners can challenge proposals',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (42,23,'Governance structure with one central authority is in place to handle
↪  changes',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (43,23,'Each participant can propose changes',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (44,24,'Consortium governance structure handles changes to the application',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (45,25,'Open governance structure to handle changes with balanced voting
↪  distributed over all participants',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (46,26,'All nodes are accepted to join the network',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (47,27,'Basic security requirements for IoT devices distributed to network
↪  participants as guidelines',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (48,28,'Extensive security requirements based on best practice, standards,
↪  regulations and classification in place for IoT devices. ',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (49,28,'Only devices which pass security requirements are accepted to join the
↪  network',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (50,29,'Dynamically adaptable security framework in place',1);
```

```
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (51,29,'Network based access restrictions based on adaptable security
↪  framework',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (52,30,'Automatic anomaly detection of potential malicious devices based on
↪  usage patterns of the device',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (53,30,'Automatic network access restriction based on anomaly detection',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (54,31,'Episodic risk assessment based on basic understanding of DLT protocol
↪  risks',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (55,31,'No processes to mitigate risks if they occur',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (56,32,'Risk analysis based on known DLT security risks from practice',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (57,32,'Focus of risk analysis is on worst-case scenarios',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (58,32,'Periodic assessment of risks and mitigation strategies in place',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (59,33,'Extensive risk assessment in place to identify possible security
↪  risks',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (60,33,'Accepted and desired risk levels are defined',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (61,33,'Mitigation strategies in place to reach acceptable risk level.',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (62,34,'Risks are detected automatically based on defined DLT protocol
↪  risks',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (63,34,'Mitigation strategies are defined and adapted when risk is
↪  identified',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (64,35,'Risks are detected automatically through a learning algorithm ',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (65,35,'Mitigation strategies automatically adapted to reach desired level of
↪  risk',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (66,36,'Keys are stored at a single point',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (67,36,'Keys are created ad-hoc when they are needed',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (68,36,'Keys are not stored in a consistent matter',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (69,37,'Key management system is in place to give access to individuals',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (70,37,'Policies defined to create keys within a project',1);
```

```
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (71,37,'Policies defined to gain access to keys within a project',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (72,38,'There are policies in place to proactively reduce risks of stolen and
↪  lost keys',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (73,38,'Storage and creation of keys handled through hardware security
↪  modules',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (74,39,'Anomalies in the network are monitored for malicious use of keys',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (75,39,'Anomalies in the key management system are monitored for malicious use
↪  of keys',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (76,39,'There are processes in place to revoke keys',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (77,40,'Identity management system is continuously improved',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (78,40,'Alternative identity systems are investigated',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (79,40,'Current key management systems are continuously improved',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (80,41,'Contents of transactions are open for other participants in the network
↪  to view',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (81,41,'No processes to reduce the amount of sensitive data on the ledger',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (82,42,'Manual process per transaction is in place to ensure no sensitive data
↪  is added to the chain',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (83,42,'Sensitive data is defined at the discretion of the user',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (84,43,'An automatic process is in place for all transactions to ensure no
↪  sensitive data is added to the ledger',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (85,43,'Sensitive data is clearly defined on a company wide basis',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (86,44,'There are measures in place to reduce the possibility of information to
↪  be gathered from the contents of transactions',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (87,44,'There are measures in place to reduce the possibility of information to
↪  be gathered from the metadata of transactions',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (88,45,'Transactional security mechanisms are continuously improved using
↪  methods like external audit testing',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (89,46,'No formal evaluation of legislation compliance has taken place',0);
```

```
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (90,46,'Evaluations that are performed are inconsistently applied, informal and
↪  incomplete',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (91,47,'After development of application a formal evaluation of compliance has
↪  been performed',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (92,47,'Some compliance controls are in place but they are not integrated with
↪  the rest of the organization',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (93,48,'Compliance with regulation is taken into account during the development
↪  of the application',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (94,48,'Compliance controls are integrated and standardized across the
↪  organization',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (95,49,'Legislative outlook has been performed to evaluate compliance with
↪  future legislation',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (96,49,'Periodic reviews are conducted to assess effectiveness and completeness
↪  of compliance controls',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (97,50,'Regular review and feedback between all involved parties are in place to
↪  ensure continuous improvement of the compliance process',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (98,51,'No formal evaluation of liability risks has taken place',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (99,51,'Evaluations that are performed are inconsistently applied, informal and
↪  incomplete',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (100,52,'After development of application a formal evaluation of liability has
↪  been performed',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (101,52,'Liability is evaluated based on agreements with ecosystem partners',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (102,52,'Liability risks are mitigated through contractual agreements between
↪  parties',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (103,53,'Liability risks are taken into account during development of the
↪  application',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (104,53,'Evaluation during development based on legal knowlegde of
↪  developers',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (105,53,'All legal risks evaluated by legal department before deployement of
↪  application',0);
```

```
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (106,54,'Liability risks are continuously monitored by legal department with
↪  direct feedback to developers',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (107,55,'Legislation is monitored to identify possible future DLT liability
↪  risks',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (108,55,'Application is developed with future legislation in mind',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (109,56,'DLT runs separately from all other applications within the company',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (110,56,'Manual input is needed to transfer information from existing
↪  systems',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (111,57,'Different connections between DLT application and existing systems are
↪  in place and separately developed',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (112,57,'Connections with existing systems are evaluated for known security
↪  weaknesses',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (113,57,'Assessment has been performed to test functionality of the
↪  connection',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (114,58,'Single secure interface is in place for existing applications to
↪  interact with the DLT application',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (115,59,'Interface with existing applications are monitored for errors',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (116,59,'Security incident detection features exist for the interfaces with
↪  existing systems',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (117,60,'Continuous monitoring of interfaces for improvements',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (118,60,'Complexity of interfaces is reduced where possible',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (119,60,'Integration infrastructure is adaptable to changes when DLT
↪  evolves',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (120,61,'Knowledge of the codebase of the application is silo-ed',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (121,61,'Codebase includes home-grown solutions',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (122,61,'Unmodifiable legacy code exists because no one knows how it works
↪  anymore',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (123,61,'Code is buggy but functions',0);
```

```
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (124,61,'Skilled engineers are not available to create application',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (125,62,'Code works and matches requirements of the application',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (126,62,'Code has duplicate solutions to the same problems',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (127,62,'Code may be difficult to understand by another software engineer',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (128,63,'Code is well documented',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (129,63,'Modern design patters are used to create code',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (130,63,'Code is readable by other software engineer',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (131,63,'Skilled engineers are available to create the application',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (132,64,'Code is modular and reusable by other DLT applications',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (133,64,'Software engineers with experience in DLT development available',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (134,65,'Quality of code can be quantitatively measured',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (135,65,'Development is continuously being improved',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (136,66,'Code is proprietary and has not been formally proven',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (137,67,'Code is audited based on functional testing',0);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (138,68,'Code is audited based on functional and non-functional testing',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (139,68,'External auditing programs are in place',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (140,69,'Development is through test-driven development principles',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (141,69,'Non-developers are able to check code with methods like model-driven
↪  engineering',1);
INSERT INTO statements(id,subMaturityLevels_id,description,required) VALUES
↪  (142,70,'Code verification procedures continuously improved with additional
↪  programs to test code when released',1);
```