LAPPEENRANTA UNIVERSITY OF TECHNOLOGY

School of Business and Management

Master's Program in Strategic Finance and Business Analytics

Master's Thesis

DIGITALIZING THE FOUNDING PROCESS OF A LIMITED LIABILITY COMPANY BY USING DISTRIBUTED LEDGER TECHNOLOGIES: A CASE STUDY OF THE PROJECT MERCURY AND ITS PROFITABILITY ANALYSIS

9th of December 2019

Mikko Mäenpää

1st Examiner: Professor, D.Sc. (Econ. & BA) Mikael Collan

2nd Examiner: Post-Doctoral Researcher, D.Sc. (Econ. & BA) Mariia Kozlova

LUT University

ABSTRACT

Author:	Mikko Mäenpää
Title:	Digitalizing the founding process of a limited liability company by using distributed ledger technologies: A case study of the Project Mercury and its profitability analysis
Faculty:	School of Business and Management
Master's Program:	Strategic Finance and Business Analytics
Year:	2019
Master's Thesis:	116 Pages, 20 Figures, 16 Tables, 6 Equations, 4 Appendixes
Supervisors:	Mariia Kozlova, Pekka Kaipio, Timo Hotti
Examiners:	Mikael Collan**,** Mariia Kozlova
Keywords:	Distributed Ledger Technology, Self-Sovereign Digital Identity, Blockchain, Digitalization, Corda, Hyperledger Indy, Decentralized Identifier (DID), Sovrin, Investment Analysis, Monte Carlo-simulation

The main objective of this case study is to illustrate how a limited liability company could be founded fully digitally based on Corda- and Hyperledger Indy-distributed ledger technologies (DLTs). The second objective of the thesis is to analyze the profitability and key risks of introducing this technology through a Monte Carlo-based investment analysis simulation. The results of the simulation are interpreted using summary statistics and visualized by the net present value (NPV), internal rate of return (IRR), and discounted payback period (DPP) distributions. Input-values for the simulation are gathered by interviewing the Project Mercury participants with semi-structured interviews. The third objective of this study is to identify and analyze future opportunities and applications for a digitalized company founding process based on the case study and investment analysis simulation.

The data for this research is gathered from Project Mercury which carried out a proof-of-concept on the possibility of this technology used in the founding process of an LLC. Project Mercury is a Finnish-based collaboration that consists of organizations from various fields that are currently involved in the founding process of a limited liability company. The development of distributed ledger technologies is in a relatively novel stage, and no evidence of DLT being applied to the founding process of a limited liability company prior to Project Mercury has been found.

Distributed ledger technologies are inspired by blockchain technologies such as Bitcoin and Ethereum, but possess different features compared to blockchains, most notably, are not fully public networks as blockchains are. As an important part of the company's digitalization process, a new kind of decentralized self-sovereign digital identity (SSI) is generated for the newly founded company based on the distributed ledger technology. This new digital identity enables, for example, the company to digitally assign representation rights for its stakeholders. In addition to that, the digital identity and the data related to it is fully owned and controlled by the company.

At the beginning of the study, a review of key technologies was made, and key concepts, blockchain, and distributed ledger technology were defined since there are no established definitions for these technologies. In the literature review previous DLT applications are introduced since this was the first time DLT was applied in the founding process of an LLC. Methodology and data chapters form the following chapters four and five. The digitalized founding process of a limited liability company using DLT and self-sovereign identity is illustrated empirically in chapter six. The results of the simulation-based investment analysis are presented in chapter seven, and the value propositions of Project Mercury for different stakeholders are discussed at the end of the chapter.

The benefits of this digitalized founding process for different stakeholders are abundant. Founders and company stakeholders are able to found the company digitally by using their bank services without any manual paper-work. Digitalized representation rights can be given to company stakeholders to represent the company on various occasions. Organizations involved in the DLT based business network can securely share and receive information related to the company and its stakeholders in real-time. Financial institutions that are part of the business network acquire cost savings, time benefits, and new business opportunities. The most important business opportunity is to digitalize and tokenize the shares of unlisted companies. In Finland alone, this could turn approximately 200 billion worth of wealth into a more liquid form.

The Monte Carlo simulation indicates that Project Mercury as an investment will be profitable on average, but the distribution between the different scenarios is wide, which indicates the riskiness of the investment and the difficulty of accurately predicting the future cash flows associated with this investment. Investments in this technology were seen more as a research and development activity. It is essential to stay updated within the field, in order to remain competitive in the future.

TIIVISTELMÄ

Tekijä:	Mikko Mäenpää
Otsikko:	Yrityksen perustamisprosessin digitalisointi DLT-teknologioita hyväksikäyttäen: Tapaustutkimus Project Mercurysta ja investoinnin kannattavuuden analyysi
Tiedekunta:	Kauppatieteet
Maisteriohjelma:	Strateginen rahoitus ja liiketoiminta-analytiikka
Vuosi:	2019
Maisterintutkielma:	116 Sivua, 20 Kuviota, 16 Taulukkoa, 6 Kaavaa, 4 Liitettä
Ohjaajat:	Mariia Kozlova, Pekka Kaipio, Timo Hotti
Tarkastajat:	Mikael Collan, Mariia Kozlova
Avainsanat:	Hajautetun tilikirjan teknologia, Suvereeni digitaalinen identiteetti, Lohkoketju, Digitalisaatio, Corda, Hyperledger Indy, Hajautettu tunniste (DID), Sovrin, Investointianalyysi, Monte Carlo-simulaatio

Tämän tapaustutkimuksen päätavoitteena on havainnollistaa, kuinka osakeyhtiö voitaisiin perustaa täysin digitaalisesti Corda- ja Hyperledger Indy -hajautetun tilikirjan (DLT) järjestelmiin perustuen. Työn toisena tavoitteena on analysoida tämän tekniikan käyttöönoton kannattavuutta ja keskeisiä riskejä Monte Carlo -pohjaisella investointianalyysi-simulaatiolla. Simulaation tulokset esitetään taulukossa ja visualisoidaan nettonykyarvon (NPV), sisäisen tuottoprosentin (IRR) ja diskontatun takaisinmaksuajan (DPP) simuloiduilla jakaumilla. Sisääntuloarvot simulaatiolle on kerätty alan asiantuntijoilta puolistrukturoituja haastatteluja hyödyntäen. Tutkimuksen kolmas tavoite on tunnistaa ja analysoida digitalisoidun yrityksen perustamisprosessin tulevaisuuden mahdollisuuksia ja sovelluksia, havainnollistavan tapaustutkimuksen ja investointianalyysin perusteella.

Materiaali tähän tutkimuksen on kerätty Mercury-projektista, joka toteutti soveltuvuusselvityksen tämän teknologian soveltuvuudesta osakeyhtiön perustamisprosessissa. Mercury-projekti on suomalaisten yritysten ja viranomaisten yhteenliittymä, joka koostuu eri alojen organisaatioista, jotka ovat tällä hetkellä mukana osakeyhtiön perustamisprosessissa. DLT teknologioiden kehitys on vielä hyvin varhaisessa vaiheessa, eikä ole löytynyt viitteitä, että DLT teknologiaa olisi aiemmin sovellettu osakeyhtiön perustamisprosessissa.

Hajautetun tilikirjan teknologia on lähtöisin lohkoketjuteknologiasta, (esim. Bitcoin ja Ethereum), mutta DLT verkoilla on erilaisia ominaisuuksia verrattuna lohkoketjuihin. Mahdollisesti suurin ero on se, että DLT-pohjaiset verkot eivät ole täysin julkisia verkkoja, kuten lohkoketjut. Tärkeänä osana yrityksen digitaalista perustamisprosessia on uudenlainen hajautettu suvereeni digitaalinen identiteetti (SSI), joka luodaan vastaperustetulle yritykselle hyödyntäen DLT:tä. Tämä uusi digitaalinen identiteetti mahdollistaa esimerkiksi sen, että yritys voi jakaa digitaalisesti edustusoikeuksia ja valtuutuksia sen omistajille ja työntekijöille. Tämän lisäksi kyseinen identiteetti ja siihen liittyvä tieto on täysin yrityksen omassa hallinnassa.

Tutkimus etenee siten, että johdannon jälkeen tehdään katsaus tutkimuksessa käytettyihin avainteknologioihin ja määritellään keskeisimmät käsitteet; lohkoketjuteknologia ja DLT-teknologia, koska näille teknologioille ei ole vakiintuneita määritelmiä. Kirjallisuuskatsauksessa esitellään aiempia tutkimuksia liittyen DLT-teknologiaan, koska DLT:n soveltamisesta osakeyhtiön perustamisprosessin digitalisoimiseen ei löytynyt aikaisempia tutkimuksia. Tutkimuksen metodologia ja data on kuvailtu kappaleessa neljä ja viisi. Osakeyhtiön digitalisoitu perustamisprosessi, jossa hyödynnetään sekä DLT-teknologiaa, että suvereenia identiteettiä on kuvattu empiirisessä luvussa kuusi. Simulaatiopohjaisen investointianalyysin tulokset esitellään kappaleessa seitsemän, sekä Mercury-projektin tuoma lisäarvoa eri sidosryhmille.

Digitalisoidun perustamisprosessin hyödyt eri sidosryhmille ovat runsaat. Käyttäjät voivat perustaa yrityksen täysin digitaalisesti kirjautumalla verkkopankkiin ilman käsin tehtävää paperityötä. Digitalisoidut edustusoikeudet voidaan antaa yrityksen omistajille ja työntekijöille, jotka voivat edustaa yritystä eri tilanteissa. DLT-pohjaiseen liiketoimintaverkostoon osallistuvat organisaatiot voivat turvallisesti jakaa ja vastaanottaa yritystä ja sen sidosryhmiä koskevaa tietoa reaaliajassa. Liiketoimintaverkostoon kuuluvat rahoituslaitokset hyötyvät projektista todennäköisesti kustannussäästöjen, aikaetujen, sekä uusien liiketoimintamahdollisuuksien muodossa. Tärkein liiketoimintamahdollisuus on listaamattomien yritysten osakkeiden digitalisointi ja niille kauppapaikan perustaminen. Pelkästään Suomessa tämä voisi muuttaa noin 200 miljardin euron arvoisen varallisuuden nykyistä huomattavasti likvidimmäksi.

Monte Carlo -simulaation perusteella, Mercury-projekti investointina on keskimäärin kannattava, mutta jakauma eri skenaarioiden välillä on laaja, mikä osoittaa investoinnin riskisyyden, sekä kassavirtojen vaikean ennustettavuuden. Investoinnit tähän teknologiaan nähtiin tutkimusyrityksessä enemmän tutkimus- ja kehitystoimintana, jossa on välttämätöntä olla mukana, jotta pysyy kilpailukykyisenä myös tulevaisuudessa.

ACKNOWLEDGEMENTS

The journey at LUT is nearing its final stop. The past several years at LUT have been a memorable time and I have been fortunate to meet wonderful people during this time and made lifelong friendships. I want to thank my fellow students for support and for all the memorable moments. In addition, I want to thank Prof. Mikael Collan as well as the personnel of LUT for high-quality education.

Carrying out this thesis has been a long process and it is rewarding to finally finish this project. I want to acknowledge the valuable support and guidance of Post-Doc. Researcher Mariia Kozlova, I greatly appreciate her contribution. I would also like to take this opportunity to thank the case company for giving me the possibility to be part of an interesting project. Especially I want to acknowledge the effort and guidance of Pekka Kaipio and Timo Hotti, for their valuable contribution.

Most of all I want to thank all the people close to me, my family and the family of my fiancé for their continuous support during the studies, which I am grateful for. Especially I want to say thank you to my dear fiancé, parents, and sister in Sweden for their invaluable support. This thesis is dedicated to all of you.

Sincerely,

Mikko Mäenpää

Vantaa, 30th of November 2019

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

API	Application Programming Interface
DDO	DID Descriptor Object
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
DPKI	Decentralized Public Key Infrastructure
DPP	Discounted Payback Period
FI	Financial Institution
FTN	Finnish Trust Network
GDPR	General Data Protection Regulation
IRR	Internal Rate of Return
KYC	Know Your Customer
LLC	Limited Liability Company
NPV	Net Present Value
PKI	Public Key Infrastructure
PoC	Proof of Concept
PoW	Proof-of-Work
SSI	Self-Sovereign (Digital) Identity

LIST OF FIGURES

LIST OF TABLES

LIST OF EQUATIONS

1 INTRODUCTION

"Everything will be tokenized and connected by a blockchain one day."

– Fred Ehrsam (2017)

There has been a lot of hype and headlines around blockchain technology and how it is going to disrupt every sector in the world (Google trends 2019, Gartner 2018). Blockchain has been identified as one of the most prominent areas of fintech, and the birth of this technology has even been compared to the birth of the world wide web, while some have praised that the impact is going to be even more significant (Beerens 2018). There has, however, so far not been many real-world applications for it.

The primary purpose of this thesis is to study how blockchain-based technologies could be utilized in the digitalization of the founding process of a limited liability company (LLC). The focus of this research is on self-sovereign digital identity and distributed ledger technology, which are the main components used in the digitalization of the founding process of an LLC (Project Mercury 2018). This study combines both qualitative and quantitative methods, and it is based on a case study of a collaboration named Project Mercury.

Project Mercury is a collaboration consisting of Finnish organizations that possess the inherent features that are required in the founding process of a limited liability company. Project Mercury involves organizations from various fields including financial institutions, tax administration authority, data service provider, IT service provider as well as registry holder of companies. The project explored how distributed ledger-based technologies could be a catalyst for transforming the formation process of a limited liability company into a fully digital one. The current end-to-end process of establishing LLC is time-consuming, highly manual, includes paperwork and is overall inefficient for the company's stakeholders as well as for the involved authorities. The project delivered a proof of concept of the distributed ledger-based company founding process which was published in May 2018. (Project Mercury 2018) The development of distributed ledger technologies is in a relatively novel stage and no evidence of DLT being applied to the founding process of a limited liability company priorly Project Mercury has been found. This thesis is written for the case

company involved in Project Mercury and is conducted from the point of view of financial institutions.

The second purpose of this thesis is to quantitatively analyze the economic benefits of investments in Project Mercury for the case company involved in the collaboration. This investment analysis is conducted by running a Monte Carlo-simulation. A simulation-based approach is used since Project Mercury (2018) as an investment holds a lot of uncertainty, and by applying simulation, different scenarios and risks can be better included in the model. Input values for the simulation are gathered by interviewing professionals within this area and by analyzing publicly available material. A Monte Carlo simulation is run by using an Excel-spreadsheet and macro programming language, Visual Basic for Applications (VBA). Results from the simulation are shown in the summary statistics and visualized by using Net Present Value (NPV), Discounted Payback Period (DPP) and Internal Rate of Return (IRR) distributions for the investment.

The tertiary purpose of this thesis is to discuss the future effects and applications of this new way to found an LLC, primarily to financial institutions and to company stakeholders, based on the illustrative case study and investment analysis simulation. In this introductory chapter, the background and motivation for the research are explained and then progressed to the research -problem, -questions and -objectives. At the end of this chapter, delimitations and the structure of the research are presented.

1.1 Background and motivation for the research

The blockchain technology was first introduced in Bitcoin´s whitepaper, which emerged to the Internet in 2008. The inventor of Bitcoin and at the same time the first blockchain carried the pseudonym called “Satoshi Nakamoto” which real identity remains unknown. (Nakamoto 2008) The price of Bitcoin and other cryptocurrencies skyrocketed in the end of 2017 and the buzz around the underlying technology - blockchain technology - was tangible (Coinmarketcap 2019).

Figure 1 displays the relative Google Trends (2019) search activity for the search term “blockchain.” Search activity related to blockchain and the prices of cryptocurrencies carries a notable resemblance to a speculative bubble graph.

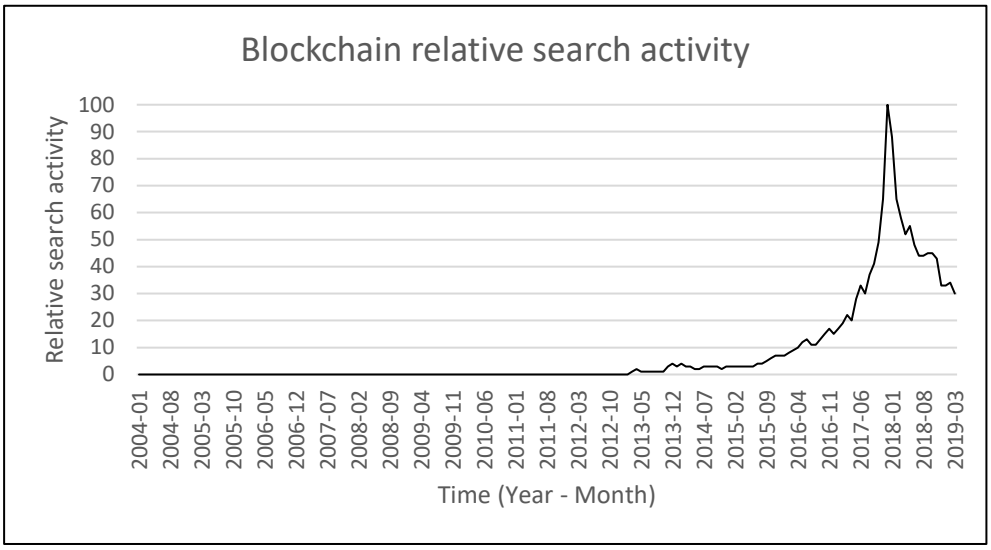

Figure 1. Blockchain relative search activity

During recent years there has been a lot of speculation around blockchain and cryptocurrencies in the air, although as so often seen with bubbles the prices of cryptocurrencies and the hype surrounding it tumbled down in 2018. (Coinmarketcap 2019) Cryptocurrencies were the first, probably the most obvious and the most used application for this innovation, and thus there is already a decent amount of academic research denominated for cryptocurrencies (Andrianto and Diputra 2018; Baur, Hong and Lee 2018; Guo and Wang 2018; Brauneis and Mestel 2018; Dyhrberg 2016; Briére, Oosterlinck and Szafarz 2015; Cheah and Fry 2015).

However, the use of blockchain technology can be extended beyond cryptocurrencies. Smart contracts, which were first used in Ethereum, made it possible to run programmable code on top of blockchain and thus added a new application layer on top of the underlying blockchain layer. (Buterin 2013) A smart contract is a computer code that contains a set of rules, and when the predetermined rules are met, the smart contract automatically executes itself without any third party (Szabo 1997). By combining smart contract and the trustless nature of blockchain technology, it opens doors for further possibilities which extend the potential use-cases beyond cryptocurrencies (Buterin 2013). However, until these days there have not been many real-world applications – only high promises - for blockchain technology. Thus, I was intrigued when I heard about Project Mercury (2018) - A real-world application for the distributed ledger technology (blockchain-based technology) which could make the

company founding process more efficient and allow a new kind of digital identity for companies which is entirely user-controlled.

Distributed ledger technologies are inspired by blockchain technologies such as Bitcoin and Ethereum but have many distinct characteristics that will be discussed in greater depth later in the technology overview (Kuo, Kim and Ohno-Machado 2017; Dewey and Emerson 2017). The main purpose for the use of distributed ledgers is to have a system that enables us to form and maintain consensus regarding the status of shared facts with different parties that *we do not fully trust* (Brown 2016). This results in a paradigmatic shift steering away from the mode of centralized silos which we have been used to. DLT provides a new way for sharing secure information, handling permissions, and as well as managing and automating processes in a decentralized way. (Project Mercury 2018)

The essential part of forming LLC fully digitally by using distributed ledger technology is to utilize a new kind of digital identity – self-sovereign identity. Self-sovereign identity is an identity that is generated and controlled entirely by the identity holder, and it is not dependent on any third parties or intermediaries. (Sovrin 2018) During Project Mercury (2018) SSI was created for both newly founded LLC as well as for the company stakeholders by using an open-source distributed ledger, more specifically Hyperledger Indy. Hyperledger Indy is specially built to be a decentralized ledger for SSI, and it enables any person, organization, or object to have a decentralized identity that they fully control (Hyperledger 2019; Project Mercury 2018). Hyperledger Indy is used as an identity management ledger since it is a public distributed ledger that everyone is able to use, but it is permissioned in a sense that allows only appropriate parties to maintain the integrity of the ledger in order to ensure proper governance (Project Mercury 2018).

Blockchain technology has been mostly studied in the context of cryptocurrencies and investing (Andrianto and Diputra 2018; Baur, Hong and Lee 2018; Guo and Wang 2018; Brauneis and Mestel 2018; Dyhrberg 2016; Briére, Oosterlinck and Szafarz 2015; Cheah and Fry 2015).

There is academic research devoted to distributed ledger technology as well, and it has been studied, especially in the context of sharing economy (Cali and Cakir 2019; Siano, De Marco, Rolan and Loia 2019; Ferraro, King and Shorten 2018) finance (Klimos 2018), settlements and clearing processes (Sekiguchi, Chiba and Kashima 2018; Manning, Sutton

and Zhu 2016; Mills, Wang, Malone, Ravi, Marquardt, Chen, Badev, Brezinski, Fahy, Liao, Kargenian, Ellithorpe, Ng and Baird 2016) but also of supply chains and trade finance (Bencic, Skocir and Zarko 2019; Sermpinis and Sermpinis 2018). When researching this research subject, no evidence of DLT being applied to the founding process of a limited liability company priorly to this has been found. This thesis is trying to suffice the apparent research gap on this topic as no prior research has emanated.

1.2 Research problem and questions

The current end-to-end process of founding an LLC is time-consuming, highly manual, includes paperwork and is overall inefficient for the company's stakeholders as well as for the involved authorities. This is due to the fact that it is not possible to share and update company information to both authorities and financial institutions simultaneously and in real-time. This is no different for the existing companies either since if the company details[1] change, the company must inform the trade registry officials and often update this information to the bank used by the company as well. (Project Mercury 2018; PRH 2019)

Distributed ledger-based technologies make it possible to share real-time verifiable information securely in between participants, and thus, in theory, could offer a solution for this use-case (Project Mercury 2018). Therefore, the aim of this thesis is to illustrate how this technology could be applied to the founding process of an LLC and to identify possible future implications. Furthermore, an additional research problem is to analyze the profitability of this proof of concept to the case company, which was part of the Project Mercury collaboration.

The research questions are derived and composed from the research problem. There are three main research questions and three sub-question questions in order to achieve a holistic and complementary view of the object of the research. All research questions will be answered and discussed at the end of the research – in the conclusion and discussion chapter.

---

1 A limited liability company must notify the Trade Register if for example the following details change: persons authorized to represent the company, board of directors, auditor, place of registered office (domicile), increase of share capital, address and contact details, procuration rights, merger, financial period, line of business, company name, managing director, or changes to the articles of association. (PRH 2019a)

Question 1: *How the founding process of a limited liability company can be digitalized with the use of DLTs?*

1.1 Which are the main DLT-ledgers used in Project Mercury, and what are these ledgers used for?

1.2 How can a self-sovereign identity be created for a limited liability company?

Question 2: *What is the estimated profitability of Project Mercury for the case company?*

Question 3: *What are the implications of Project Mercury for different stakeholders?*

3.1 What are the future implications and opportunities of Project Mercury?

The first main and sub-research questions will be covered and answered in chapter six based on the case study of Project Mercury. The second research question will be covered in the quantitative part, chapter seven, based on the investment analysis simulation. The results will be interpreted by using summary statistics and visualized with NPV, IRR, and DPP distributions. The investment analysis simulation is conducted from the point of view of a financial institution. The third research question can be answered at the end of chapter seven based on the case study and investment analysis simulation.

1.3 Focus of the research

It is essential to have a focus for research to manage the scope of the study (Simon, 2011). This thesis is constituted upon a business perspective, and the technical details presented are limited to what is beneficial for the scope of this thesis. This research includes some cryptography that is related to the public key infrastructure (PKI) and decentralized public key infrastructure (DPKI) but does not go deeply into the cryptography used in blockchain or distributed ledger technology.

Blockchain and DLT technologies are both broad concepts and in premise can be used for various different applications (Cali and Cakir 2019; Siano et al. 2019; Bencic et al. 2019; Ferraro et al. 2018; Klimos 2018; Sekiguchi et al. 2018; Sermpinis et al. 2018; Manning et al. 2016; Mills et al. 2016). In this study, there is no research related to other possible blockchain or DLT applications other than used in Project Mercury. This study is exclusively focusing on how LLC can be founded fully digitally by using distributed ledger technology.

In this research paper, the blockchain technology and the DLT-technology are first defined and reviewed in the theoretical framework and technology overview chapter. This review is essential to this study, as DLT-technology act as a backbone for Project Mercury. The blockchain technology is covered in the technology overview chapter, however to no further extent than that. The focus thereafter lies solely on the DLT-based technologies, more specifically on Hyperledger Indy and Corda (Hearn 2016, 4-5, Hyperledger Indy 2019) Hyperledger Indy is covered since it is used as a ledger for self-sovereign decentralized digital identity, and Corda is discussed since it is used for transaction processing in the network (Project Mercury 2018). All other DLT platforms and possible use-cases for DLT technology are excluded from this research.

Figure 3 seen below exemplifies delimitations in this thesis and the relationship between different research objectives. As can be seen from Figure 3, the main focus in this research lies in DLT-based technologies, but the blockchain technology is partially covered since there is a strong linkage between these technologies.

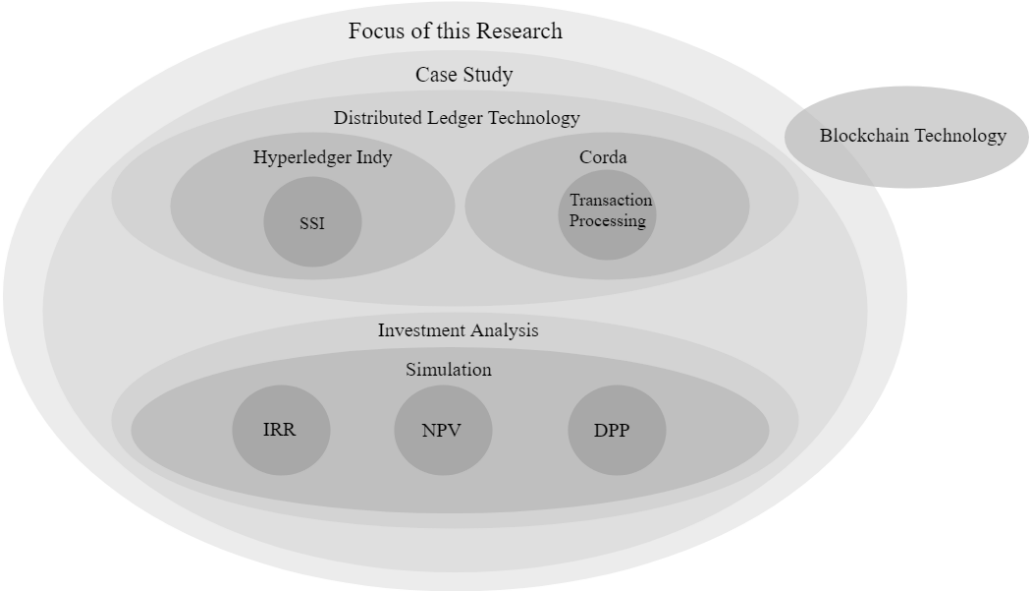

Figure 3. Focus of the research

The quantitative part of this thesis is conducted by using Monte Carlo simulation-based investment analysis and delimitations include that the results are analyzed by using IRR, NPV, and DPP distributions.

SSI is an essential part of the digitalizing the company founding process and this, it constitutes the core of this study. To achieve a fully functioning SSI, there need to be decentralized identifiers (DID) for identity holders. (Reed, Sporny, Longley, Allen, Grant and Sabadello 2019) Project Mercury (2018) did not apply pairwise pseudonym DIDs, due to that it would have required additional resources with the increased workload, and it would have added to the complexity of the proof of concept. Pairwise pseudonym DIDs are created to increase privacy and reduce the correlatability of identity holders (Sovrin 2018). In the chapter theoretical framework and technology overview, there is a review of DIDs and their use.

In theory, the network developed by Project Mercury (2018) is not geographically limited to be used only in Finland since it is based on open-source Corda and Hyperledger Indy technologies. However, although this network could be used globally, in this study, it is studied in the context of being used in between Finnish organizations since the network must comply with the Finnish law.

1.4 Research objectives

Research objectives are discussed in order to understand what will be attained by the study and to elucidate how the study may be implemented as well as to justify the methodology used. This study is a combination of qualitative and quantitative research methods to achieve the research objectives presented in Figure 2.

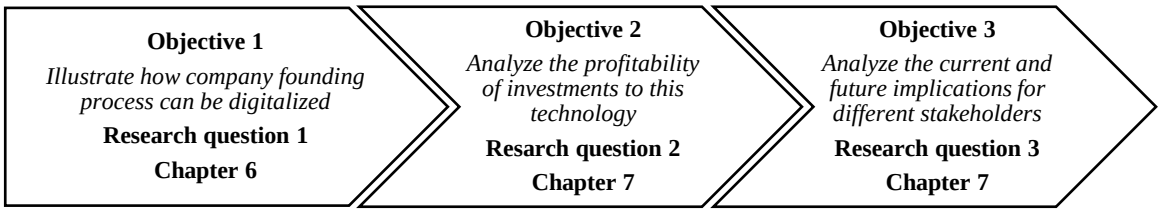

Figure 2. Research objectives

The first research objective is to illustrate how an LLC company can be founded entirely digitally using blockchain-based technologies. This is achieved by using a case study as a research method. A case study is a qualitative method, and it entails an in-depth and detailed examination of the research subject - Project Mercury. Based on the case study, it is possible to construct a clear and deep understanding of the studied objective. Project Mercury is a unique concept, and according to the collaboration, it was the first time when DLT was applied in the founding process of an LLC. A case study as a research method is selected since there are no other sources of information related to this research subject. Data for this case study is gathered by participating in Project Mercury meetings, utilizing provided case material, and interviewing experts within the project. Based on this data and the used methodology, is it possible to analyze and illustrate the digital company founding process by utilizing distributed ledger technologies.

The second objective is to analyze the profitability of Project Mercury for the case company involved in the collaboration. The objective is to quantitatively analyze the profitability and risk associated with the investment by using Monte Carlo simulation. Input values for the simulation are gathered by interviewing experts that were part of Project Mercury (2018) collaboration. A simulation-based approach is used in this thesis since there is a lot of uncertainty related to this investment. This is due to the fact that Project Mercury acquired the opportunity to accomplish something that has never been done before and additionally to that the project is still in a PoC-stage which makes it even more challenging to estimate the profitability of a production-ready service. Results of the simulation are interpreted by using summary statistics and NPV, IRR, and DPP distributions for different scenarios.

The third research objective is to analyze the current and future implications of this new founding process for different stakeholders in Project Mercury. The research method is a combination of both quantitative and qualitative analysis. It is based on a literature review, case study (interviews of experts, meetings, and materials provided by the Project Mercury) as well as the investment analysis simulation. Based on this diverse data, it is possible to interpret and analyze the future implications for both company stakeholders as well as for the financial institutions.

1.5 Structure of the research

The first chapter – Introduces the research subject of this research and covers the background and motivation for the research. Research questions derived from the research problem are introduced as well. The objectives of the research are discussed and presented, after the research questions. The delimitations of the research and structure of the research are introduced at the end of the introduction chapter.

The second chapter – is focused on the theoretical framework of this research and provides an overview of the technologies used. The chapter starts by introducing and defining decentralized ledgers, which includes the distributed database, blockchain technology, and the distributed ledger technology. A more profound overview is performed for the technologies used in Project Mercury, which include Corda and Hyperledger Indy. The concept of self-sovereign identity and the technical aspects of is reviewed at the end of chapter two.

The third chapter – is the literature review, and it presents the previous academic research related to DLT and SSI. Furthermore, this chapter provides a literature review related to the methodologies of this thesis. This involves a review of a case study, Monte Carlo-simulation, profitability analysis, consensus decision-making, and interviews.

The fourth chapter- is the methodology and data chapter for the illustrative case study. The subject of the research, Project Mercury, is presented as well as the illustrative case study as a methodology. In addition, the data for the illustrative case study is presented.

The fifth chapter – is the methodology and data chapter for investment analysis simulation. The methodology used in the investment analysis simulation, Monte Carlo simulation, is presented as well as the input-values for the simulation are described. The data used in this research is presented as well as the calculation methods for NPV, IRR, and DPP values.

The sixth chapter – represents the qualitative empirical part of this thesis. This includes an illustrative case study on Project Mercury and introduces the distributed ledger-based fully digital founding process of a limited liability company. This chapter combines the technologies presented earlier and exhibits how these technologies could be utilized to digitalize the founding process of an LLC.

The seventh chapter – is the quantitative chapter, and it presents the Monte Carlo simulation-based investment analysis for Project Mercury. The results and profitability of investments are visualized by using NPV, IRR, and DPP distributions. Input values for the simulation are gathered by interviewing professionals and by using estimations based on the material provided by Project Mercury. Consensus decision-making modeling is used for achieving the consensus for the input values. At the end of the chapter, future impact and applications of Project Mercury are discussed.

The eight chapter – is the conclusion and discussion chapter. In the conclusion chapter main and sub research questions are answered, and critique and the limitations for the research are presented. At the end of the chapter, future research objectives are discussed.

The illustration of the structure of this thesis and answers to research questions can be seen in Figure 4 below.

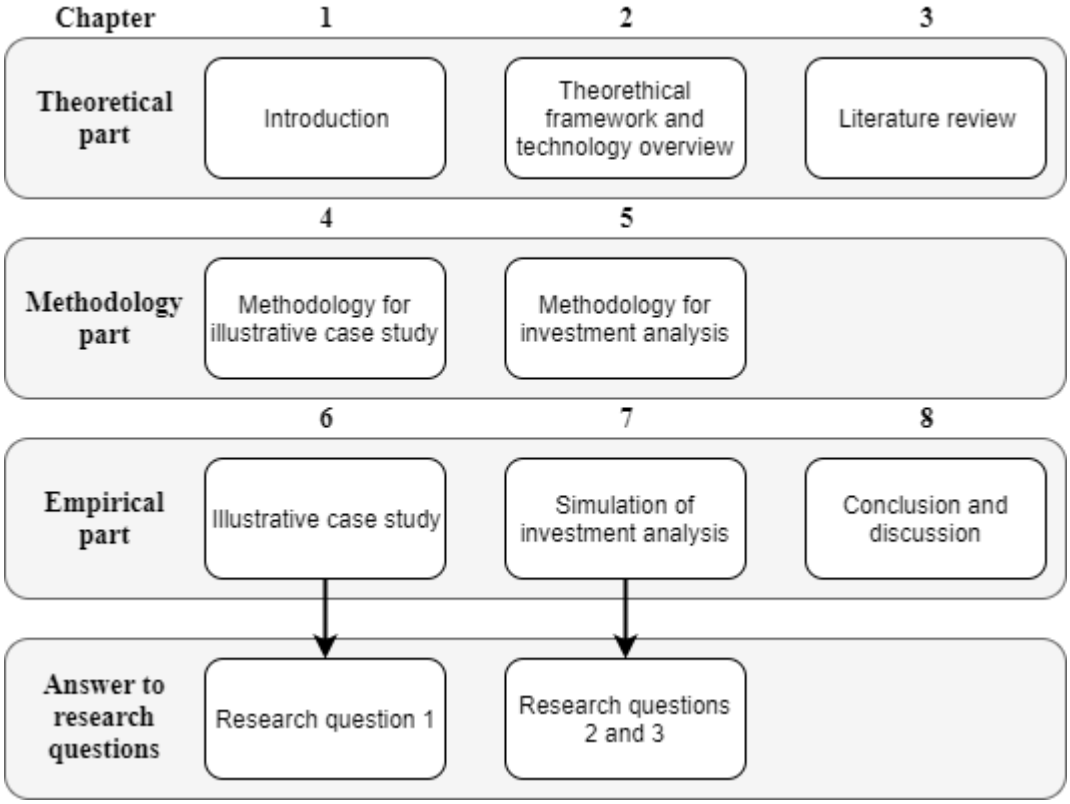

Figure 4. Structure of the research

2 THEORETICAL FRAMEWORK AND TECHNOLOGY OVERVIEW

The theoretical framework of this research consists of a review of the technologies used in Project Mercury. Blockchain and distributed ledger technologies are relatively new innovations and broad concepts, thus a technological overview is in place.

In this chapter, a basic overview of distributed technologies is conducted to understand the essential differences and limitations between different distributed ledgers. There is no general or widespread definition for blockchain and distributed ledger technologies since these are relatively new technologies and there are various different DLT and blockchain frameworks. (Jeffries 2018). This might lead to a misuse of these terms, and thus these technologies are often confused with each other. For this reason, blockchain and distributed ledger technologies are defined in this study to achieve a common language. It should be noted that the terms used in this study are for the purpose of this paper and terms may vary on different occasions.

The theoretical framework of this paper is based on the overview of distributed systems, and it starts in chronological order from the oldest technology to the newest one. Figure 5 illustrates the evolution of distributed technologies.

Figure 5. The evolution of distributed systems

A distributed database is involved in the technology overview to perceive the main differences between different distributed systems. A distributed database is the oldest of the presented distributed systems, and it can be used as a benchmark when compared to blockchain and DLT systems (Hileman and Rauchs 2017). Blockchain as technology was first introduced in 2008 with Bitcoin and thus is defined after the distributed database (Nakamoto 2008). DLT is the latest of these technologies, and there is a more detailed overview since it is an essential part of Project Mercury (2018). This includes a more detailed overview of Corda and Hyperledger Indy distributed ledgers. Technology overview for SSI is conducted after the Hyperledger Indy since it acts as a distributed ledger for self-sovereign identity (Sovrin 2018). SSI includes decentralized identifiers and decentralized descriptor objects which will be part of this technology overview (W3C 2019). Figure 6. shows the chronological progression of this chapter and the main contents in this theoretical framework.

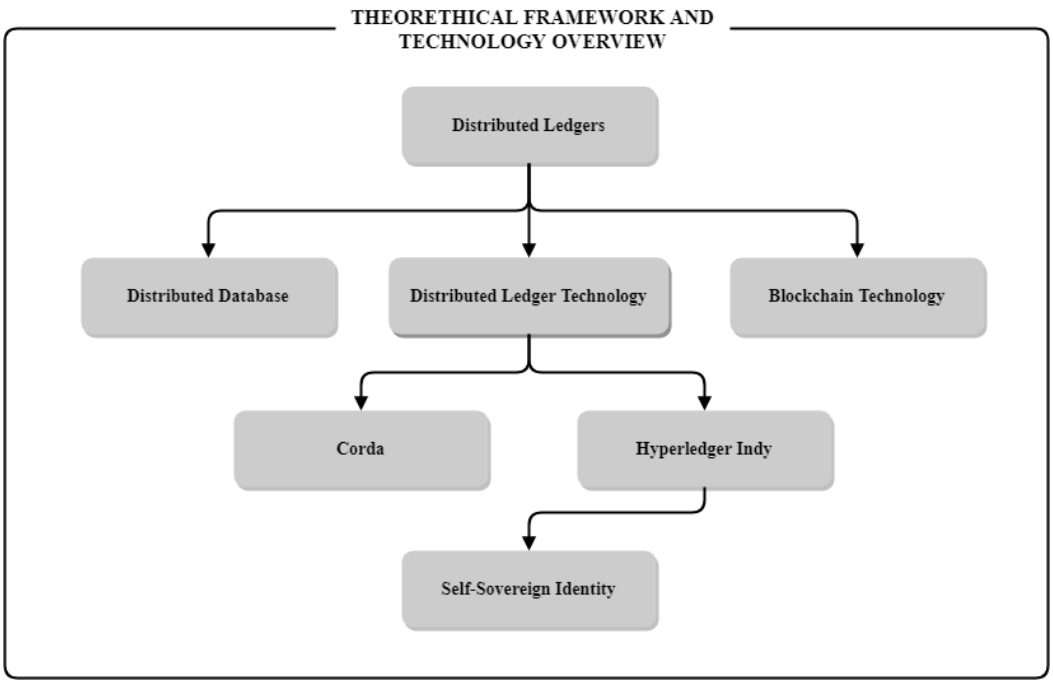

Figure 6. Theoretical framework and technology overview

2.1 Distributed database

A distributed database is a database that consists of multiple nodes that are usually owned and controlled by a single organization. A distributed database can also be controlled by

numerous organization which has high mutual trust amongst each other. The nodes in the distributed database architecture can freely share data between each other by using replication and duplication to maintain accurate records about the state of the shared facts. The nodes within the distributed database architecture can trust each other since they are under the control of a single organization or organizations that have high mutual trust. Due to this trust model, nodes can trust data received from the other nodes inside the trust boundary, but data coming outside from the trust boundary needs to be validated. Access to the database is controlled by the organization, and therefore the distributed database model assumes that nodes can exchange information freely. The data can be trusted since the data is moving within the company or trusted parties. (Lake and Crowther 2013, 36-37; Brown 2016)

Figure 7. Illustrate the trust boundary between the nodes and the outside world. Nodes inside the trust boundary can trust each other since they are under the control of a single entity or entities that have very high mutual trust. (Brown 2016)

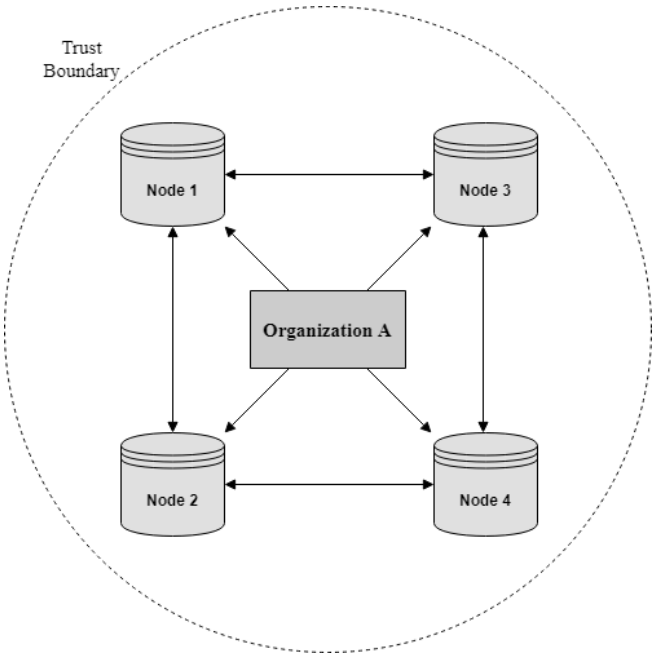

Figure 7. Distributed database structure

The advantage of the distributed database is that it is highly scalable compared to the blockchain and DLT networks since lighter consensus algorithms can be used. However, if organizations that do not fully trust each other need to maintain their records, in synchrony

with other organizations, this architecture is not sufficient. For this reason, this architecture is not usually used among organizations that do not fully trust each other. (Brown 2016)

2.2 Blockchain technology

Blockchain technology was first proposed by pseudonym Satoshi Nakamoto in Bitcoin´s whitepaper *"Bitcoin: A Peer-to-Peer Electronic Cash System"* which emerged on the Internet in 2008 (Nakamoto 2008). It should be noted that Nakamoto (2008) did not mention the term "blockchain" itself in the whitepaper but described the principles of Bitcoin – which was the first cryptocurrency based on blockchain technology. The identity or identities behind the pseudonym Satoshi Nakamoto is still unknown.

The name "blockchain" is most likely derived from the functioning of a blockchain: Transactions that have occurred in the peer-to-peer network within a predetermined time-period are bundled together and formed into a block. The new block is then cryptographically linked to the previous set of blocks, forming a chronological sequence of blocks in a chain, - the so-called blockchain. (Nakamoto 2008) The blockchain ledger is often described to be immutable, but it is dependent on the hashing power of the network and a degree of decentralization. (Sultan, Ruhi and Lakhani 2018) There are estimated to be hundreds of different blockchains in existence (Coinmarketcap 2019).

Blockchains are public systems in the same way that the Internet is public (Sovrin 2018). In practice, this means that anyone can use blockchain by sending transactions in the network and maintain the integrity of the ledger by participating in an action called "mining" (Qin, Yuan, Wang 2018; Dwyer 2015; Bollen 2013). Transactions occurring in a blockchain network are usually settled almost in real-time, and all transactions are visible to all users of the network. Anyone can use or read the ledger since blockchains are public systems and there are no authentication procedures. There is no standard way to know or verify the users of a blockchain due to the lack of "Know Your Customer" procedures. Blockchain is described as a pseudo-anonymous system since we can see and examine the public addresses of users, but we do not know the identities of the users. (Sharma 2018; Sultan et al. 2018) Logically, if we do not know the identities or motives of the users, those cannot be trusted. Therefore, there needs to be an incentive layer build-in to incentive unknown and untrusted participants to work according to the predetermined rules. (Buterin 2017; Nakamoto 2008)

This incentive layer is known as “cryptoeconomics”. In the simplest term cryptoeconomics means using cryptography to prove properties that have happened in the past and use economic incentives to encourage participants to act in the desired way in the future. (Buterin 2017a). The desired way in the context of blockchains means acting according to the rules of the blockchain network. If miners, the book-keepers of the blockchain, follow the rules of the network, an economic incentive – cryptocurrency - which is used in the network will be given to miner(s) as a reward if they are able to solve the block. To solve a block, miners need to spend their computing power – which means spending their resources. If miners are not following the rules of the network and are acting maliciously they will not get the block reward and are thus wasting their computing power which cost resources. This process is also known as a Proof-of-Work (PoW) or Nakamoto consensus referring to the pseudonym used in the Bitcoin’s white paper. For this reason, there is cryptocurrency built into the public blockchain – to incentive unknown and untrusted participants to work according to the pre-determined rules. As long as miners are competing to find a block and none of the miners have more than 50 % percent of the computing power of the network, the network remains secure. However, if a malicious actor gains more than 50% of the computing power in the network they can “double-spend” their transaction which means spending their cryptocurrency more than once. This is the fundamental economic model that makes public blockchains secure. (Dwyer 2015; Bollen 2013; Nakamoto 2008)

Due to the cryptoeconomics users of the blockchain can work together to generate and maintain the ledger in a decentralized manner, without the need for involved parties to know or trust each other. For this reason, so-called third parties can be precluded from verifying events/transactions. Trust arises because all events are stored in the blockchain, and it is difficult to tamper or change transactions afterward. (Swan 2015, preface)

Blockchains can be divided into two different categories based on their features. “First-generation blockchains” have only one primary function: to move value in the form of cryptocurrency. First-generation blockchains were revolutionary in the sense that individuals were able to move value between each other securely without trusted third parties (e.g. financial institutions) to act as a middleman. For example, Bitcoin, Monero and Litecoin can be seen as first-generation blockchains. (Prybila, Schulte, Hochreiner and Weber 2017)

The “Second-generation blockchains” can be seen as an evolution compared to the first generation blockchains. The second-generation blockchains have so-called “smart-contract”

functionality build-in which extended the capabilities of blockchain technology beyond simple cryptocurrency transactions. These second-generation blockchains enable users to build decentralized applications that are run by smart contracts. (Buterin 2013) Smart contracts are enforceable digital contracts that execute themselves when certain programmed conditions are met (Szabo 1997). The digital tokenization of assets with smart contracts was also possible with the second-generation platforms (Buterin 2013). The first so-called second-generation smart contract- platform and currently the largest one, measured by market cap, is Ethereum (Liu, Yu, Chen, Xu and Zhu 2017). Ethereum's genesis (first) block was mined at the end of July in 2015 (Etherscan 2019).

The term blockchain in this thesis is defined as a decentralized ledger that is available for anyone to use, just like the Internet is a public network open to everyone. However, for a ledger to be classified as a blockchain, there needs to be a cryptocurrency build-in since it acts as an incentive for unknown miners to maintain the integrity of the ledger. According to these definitions, for instance, Ethereum and Bitcoin are "blockchains" since they meet the criteria, but permissioned ledgers which are forked from the public blockchains do not meet these criteria.

There are, however, several disadvantages related to blockchain technology which could hinder the adoption of this technology. The same properties that make blockchain secure and decentralized make it also less scalable than other distributed ledgers. (Buterin 2017b) Figure 8 represents the scalability trilemma.

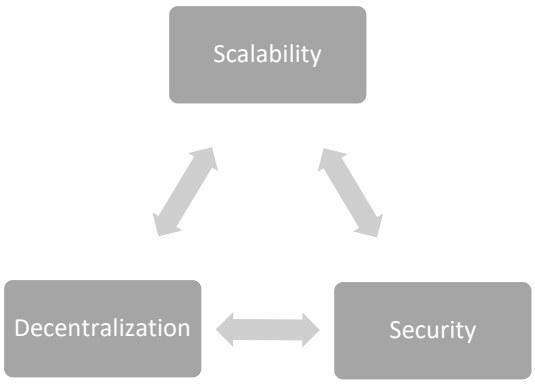

Figure 8. Scalability trilemma

The Achilles heel with distributed technologies is a trade-off called "scalability trilemma," which was described by the inventor of Ethereum, Vitalik Buterin (2017b). The trilemma

claims that distributed technologies can only have a maximum of two properties out of all three. The properties are decentralization, scalability, and security. In short, it is very difficult to achieve a scalable blockchain without sacrificing one or two of all three properties. (Buterin 2017b) According to Chauhan, Malvuya, Verma, and Mor (2018) scalability is one of the main reasons why public blockchains are not ready for large scale commercial use. There are multiple different scalability solutions in development for different blockchains. Therefore, this might be solved in the future, due to technological development (Buterin 2017b).

There are also various other hurdles or characteristics which might hinder the adoption of this technology. Data privacy is one major concern related to blockchain technology. Blockchains are open systems, therefore, all transactions are broadcasted and stored to all nodes in the network. (Androulaki, Karame, Roeschlin, Scherer and Capkun 2013) All users in the network can see the occurred transactions and data cannot be revoked after it is written on the ledger (Hoffman, Wurster, Eyal and Bohmecke-Schwafert 2017). However, this can also be seen as an advantage since it is not possible to manipulate or tamper data after it is written on the ledger. Sensitive data can always be encrypted before it is written on the ledger, but as history has proven even the strongest encryptions might be broken in the function of time. (Dougherty 2008) Therefore, it would be better that sensitive data is only shared with participants to whom it belongs.

Some other concerns related to blockchains are their governance. All users can suggest changes to the blockchain protocol since blockchain is an open-source code. However, the changes are only implemented if the majority of the “miners” agree with the changes. The blockchain can split into two different chains if there is no consensus related to the implementation of changes. This event is known as a hard fork, and there are various examples of hard forks occurring in blockchains. (Voshmgir 2017; Devlin and Guinan 2017)

The regulation related to blockchain technology is often unclear and it varies across different countries since blockchain is a new technology. It can be expected that the regulation related to this technology would mature and unify across countries when the technology matures, (Devlin et al. 2017)

Blockchain can be seen as a secure, tamper-proof, distributed, and a censorship-resistant computing platform for smart contracts (Buterin 2013). Smart contracts often need data from

external links to work. However, the full potential of smart contracts is not reached if there is only one single data link connected to a smart contract. A single data link or source can be tampered, which would lead to false input values for the smart contract and then to false output values. To get accurate data for smart-contracts one possible solution would be to use multiple data sources and follow the consensus of these values. Thus, a single malicious data link would not hinder the use of a smart contract. (Ellis, Juels and Nazarov 2017)

Blockchain is based on DPKI which means that the secure management of cryptographic keys is essential (Allen, Brock, Buterin, Callas, Dorje, Lundkvist, Kravchenko, Nelson, Reed, Sabadello, Slepak, Thorp and Wood 2015). Especially the management of private key(s), which is used to sign transactions (Nakamoto 2008). If a malicious actor gets access to the private keys, the attacker can steal all the digital assets associated with the cryptographic account. Unfortunately, there is no way to recover funds after this since there is no trusted third party that could cancel or reverse the transaction after it is initiated. There are many examples related to poor key management, which have caused severe financial losses to the owners. (Hu 2019)

Due to these characteristics and hurdles, it seems that blockchain technology generally is not yet ready for a large scale commercial use. However, due to the technological development and establishment of this technology, this can change in the future.

2.3 Distributed ledger technology

Distributed ledger technology is the most recent type of technology from the field of distributed systems. It should be noted that there is a vague usage of terms within this field, which can create controversy regarding the definition of this technology (UK Government 2016, 15). DLT technologies are often mixed with blockchain technology since there is no established definition for distributed ledger technology. Blockchain can be seen as a type of distributed ledger, and it can be argued that all blockchains use distributed ledgers, but distributed ledgers do not necessarily use blockchain. (Belin 2019) In the academic literature, distributed ledger technology can be sometimes quoted as a permissioned- or private-blockchain as well. In this thesis, however, private- and permissioned- blockchains fall under the umbrella term of distributed ledger technology (Kuo et al. 2018). The usage of various different terms is due to the fact that it is difficult to define this technology

precisely and because there is not only one type of DLT but various different DLT frameworks.

The main difference between DLT and blockchain technology is that DLT does not need a build in cryptocurrency or PoW-algorithm to work since there is trust between the operators of the network and the users of the network are known. Blockchain is a completely open system, and the users in the network are unknown and untrusted, but in DLT the right to read and write the ledger can be, and usually is, restricted to chosen and trusted parties. (Mohanty 2019, 17)

The spark to develop distributed ledger technology emerged since the blockchain technology was seen as a potential technology but in its current form was not able to satisfy the needs of existing businesses, partly due to the restrictions discussed in the chapter 2.2 (Mohanty 2019, 43 – 44; Brown 2018, 18-19; Hearn 2016, 4-6). There is a wide variety of different kinds of DLT technologies in existence, and the technological decision can wildly vary between different DLTs (Mohanty 2019, 42 - 46).

Distributed ledger technology is a way to replicate and share a ledger between multiple parties in a way that consensus is achieved. There is no central authority that tracks the records, and thus there is no “single point of failure” as it is in traditional databases. This results in a reliable source of data that is robust to system failures and that cannot easily be tampered. DLT allows parties to maintain shared, synchronized and accurate records without having to trust each other fully since the data is not controlled by a single entity. Different kinds of consensus algorithms can be used to achieve consensus about the state of shared information. In practice, the ability to read or write the ledger is also restricted only to participants that are at least partially trusted. (Hearn 2016, 4-6; UK Government 2016, 5-6)

Figure 9. replicates the real-world situation which can be present between different organizations that are conducting business with each other. Organizations (A, B, C, D) have their own databases that they fully control, which means that access to the database is restricted and all incoming information is validated. Organizations are conducting business with each other, but they cannot fully trust their counterparts. Hence, organizations want to store, validate and process their own data by using centralized databases that they fully control. This leads to trust boundaries separating the organizations. Trust boundaries hinder the information flows between organizations and can lead to fragmented and siloed data.

The data flows between different organizations might become opaque. This is one of the most fundamental problems related to conducting business with different parties. Since transacting parties are moving value with each other they need to have a consistent view of the shared data and have a consensus with that. This is the underlying problem that DLT is designed for: "*To break down the data silos and let data and assets to move between different parties without any friction and to eliminate the process of duplication and reconciliation of data.*". (Brown 2016)

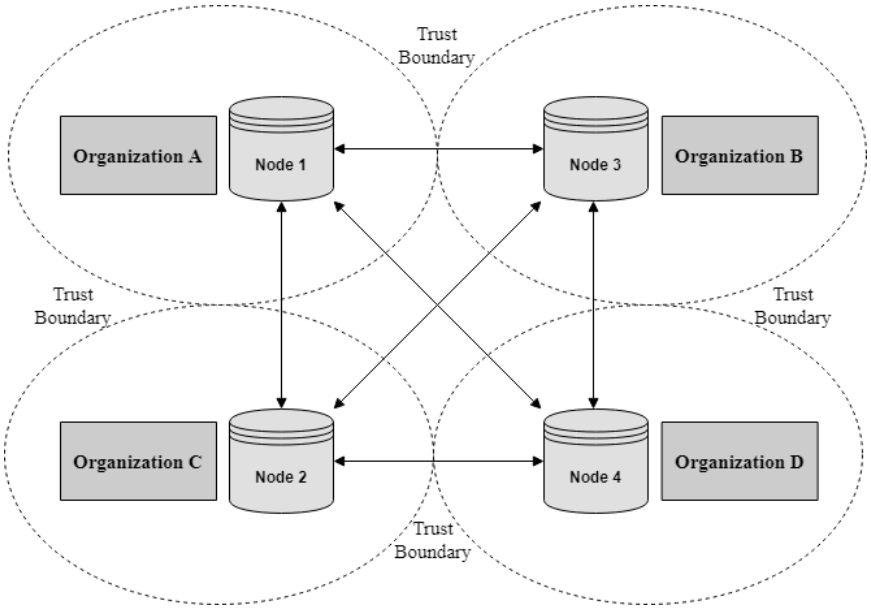

Figure 9. Trust boundaries between organizations

DLT is not as trust-free as blockchain technology since it is not using cryptoeconomics to incentive users to work according to rules of the network (Buterin 2017a). Cryptoeconomics is not used since users in the network are identified and at least partly trusted, hence there is no need for cryptoeconomics (Brown 2018). The disadvantage of this is that there is a trust boundary between the ledger and the outside world. In premise all users need to be validated before they can join in the network, thus the name permissioned ledger sometimes used with DLT. Blockchain, on the other hand, is a public ledger and everyone can join and start using the ledger without the need to ask permission, thus it is sometimes referred to as a permissionless ledger (Kuo et al. 2018). Blockchain is sometimes compared to the Internet since it is an open system in which anyone can join, whereas DLT is often compared to Intranets since the ability to read and write ledger can be restricted (Harju 2017). DLT is not completely immune to the hurdles affected by blockchains. However, it is less affected by

those since parties validating the transactions are known and trusted and there is no need for the inefficient PoW-algorithm (Brown 2018, 19).

One of the largest and most well-known open-source DLT-consortiums is built around Corda and various Hyperledger frameworks hosted by Linux Foundation (Project Mercury 2018). Hyperledger Indy framework and Corda, are the distributed ledger technologies used in the Project Mercury (2018). These specific technologies are studied more profoundly in the following chapters. According to Sovrin (2018), SSI could not exist without decentralized ledger technology. This is due to the decentralized root of trust that DLT-technology provides and therefore it acts as a catalyst and enabler for SSI (Sovrin 2018).

The term distributed ledger technology in this thesis is defined as follows. A ledger to be classified as a DLT there needs to be a distributed ledger used amongst entities in the network. Maintaining the integrity of the ledger is restricted to trusted parties, but the access to use and read the ledger can be open for anyone. There does not need to be built-in cryptocurrency because the validation of transactions is restricted to trusted parties. According to these definitions, for instance, Corda and Hyperledger Indy frameworks qualify to be classified as a distributed ledger technology but not as a blockchain technology since there is no need for cryptocurrency to incentive parties that validate the transactions.

2.3.1 Corda

Corda is an open-source DLT-platform developed by R3 led alliance which consists of an ecosystem of more than 300 participants from various fields (R3 2019a). Corda –published and open-sourced its codebase on November 30th, 2016 (R3 2019b). Corda is especially trying to solve the issues related to recording and enforcing business agreements between financial institutions which could automate the cross-organization business flows. Corda does not claim to be a general-purpose blockchain platform for everyone such as Ethereum. Corda is inspired by blockchain technology, but it does not have any built-in cryptocurrency and nor does it use or store data in blocks. Corda especially underlines the issues related to scalability, privacy, and governance. (Brown 2018)

The usage of terms related to Corda from the R3 alliance can be seen as contradictory since Corda's technical white paper especially deny the use of blockchain, by stating: "*There is no block chain*" and present it as a "*decentralized database*" (Hearn 2016, 4-5). In addition,

"Corda introductory white paper" they state that "*Corda is a distributed ledger platform for recording and processing financial agreements*" (Brown, Carlyle, Grigg and Hearn 2016). However, Corda homepage defines Corda as "*An open-source blockchain platform for businesses*" (Corda 2019a). This signifies the need for more precise and more established terminology in this space. According to the definition used in this thesis Corda is classified as a distributed ledger technology.

Corda is trying to streamline business transactions and change the way businesses transact today and move away from the isolated centralized silos by implementing a new global logical shared ledger that records the financial events and processing of business logic. By global ledger Corda is meant to be a reliable single source of truth open for anyone, but the transactions that take place are only happening point-to-point between the involved parties. This is also known as partial visibility and is probably the single most notable difference to blockchain technology. The partial visibility solves the issues related to data privacy which was discussed in the blockchain chapter. (Brown et al. 2016, 4, 8)

State Objects are one of the key concepts in the Corda ledger. The state object is a digital document that describes the existence, current state, and content of the agreement between involved parties and is only shared between the parties that have the permission to see it. Corda's state objects are governed by a machine-readable Contract Code. Corda relies heavily on cryptographic hashes to identify parties and data, and the ledger is a set of immutable state objects. The objective of Corda is to ensure that all parties agree or remain in consensus about the state of the contract as it evolves. To update the state object, parties need to make a transaction which consumes the existing state objects and produce new state objects. This feature is borrowed from the Bitcoin protocol and known as the UTXO (An Unspent Transaction Output) model. (Brown et al. 2016, 8; Brown 2018, 8 - 10)

Consensus over a transaction is only reached in the level of transacting parties since the transaction is sent only between the participants, whereas most "blockchain" platforms reach a consensus within the ledger level. Thus, participants in Corda sees only a small fraction of the overall data sent in the system as a whole. Corda's consensus is reached by using cryptography and notary services. Corda is not using a blockchain, and there are no "blocks" where transactions are bundled in as it is in "traditional" blockchains. (Brown et al. 2016, 9 – 10; Hearn, 2016, 29 – 33; Brown 2018, 16)

Corda's "*notary services*" provide transaction ordering and timestamping services which are done by "miners" in traditional blockchains. Notary services ensure that no double-spending of transactions is happening. There can be one or more notaries, and notaries are expected to be run by multiple mutually distrusting parties. There can be different consensus algorithms (e.g. BFT, Raft) depending on the use-case and Corda does not tightly integrate any specific one. When there is more mutual trust among the users, and high throughput is needed, lighter consensus-algorithms are sufficient. Transacting parties in the Corda network are known and malicious activities can be penalized by real-world legal systems thus lighter algorithms may be used. However, this is dependent on the situations, and different trade-offs might be preferred in different use-cases. Transactions in the Corda network are finalized when notary service has signed them, whereas blockchain systems offer a probabilistic finality. The nodes of notary services might use Intel SGX (Software Guard Extension) in the future which will increase the trustiness of notary nodes because of increased hardware protection. (Hearn 2016, 29 - 31; Brown 2018, 16 – 17)

Corda's main approach to solving the challenge related to data privacy is not to broadcast the transactions globally. Only the parties that are involved with the transactions and the notary service are able to see the transactions. This is also probably the single largest reason which separates Corda from other DLTs and blockchain ledgers. Corda might also implement zero-knowledge proofs (ZKP) in the future which would greatly increase the privacy of transactions. ZKP allows peers to validate data without ever seeing the content. There are various other privacy improvements proposed as well including key-randomization and graph pruning to name a few that enhance the privacy of the Corda network. (Brown et al. 2016, 10, 14; Hearn 2016, 12, 36, 51, 52)

The partial visibility which solves the data privacy is also the main solution for scalability. Since nodes need to proceed only the transactions that involve them, only a fraction of the transactions occurred in the whole network are proceeded by a single node. Therefore, direct comparison to other decentralized ledgers is not possible, and maximum capacity (e.g. transactions per seconds) is not meaningful to measure. (Hearn 2016, 48 – 51)

2.3.2 Hyperledger Indy and Sovrin Foundation

Hyperledger is an open-source global collaboration that creates cross-industry distributed ledger technologies and is hosted by the Linus Foundation. Hyperledger was launched in 2016 with 30 founding corporate members. (Hyperledger 2019a; Hyperledger 2019b)

Hyperledger currently has five different distributed ledger frameworks; Sawtooth, Iroha, Fabric, Burrow, and Indy. Each of these frameworks has different characteristics for different use-cases (Hyperledger 2019e). In this technology overview, Hyperledger Indy is the only framework that is going to be reviewed since it is used in the Project Mercury as a ledger for self-sovereign identity (Project Mercury 2018). According to the Hyperledger (2019c), Indy is a distributed ledger especially built for decentralized digital identity, and it enables any entity to have a decentralized identity that is controlled by the identity holder. There is no native cryptocurrency build-in the Hyperledger Indy, and it is permissioned in the sense that only trusted parties can validate the transactions. Therefore, Indy is defined as a distributed ledger in this study. (Hyperledger 2019c)

Indy can be seen as a *public permissioned distributed ledger*. This implies that anyone can access the ledger but the validation, or maintaining the integrity of the ledger, is done only by the trusted pre-chosen parties, so-called “Stewards”. Indy is seeking to be a global identity network, thus it is a public ledger which anyone can access. Table 1 shows the main differences between Ethereum, Corda and Hyperledger Indy. (Windley 2017)

Indy has a relationship within the Sovrin Foundation since Sovrin is a public utility for identity and it is built on top of Indy’s codebase (Hyperledger 2019d). Users can download and install Sovrin packages which integrates the Sovrin’s governance and trust framework. However, it is possible to use Indy node for different identity networks as well. (Hyperledger 2019d)

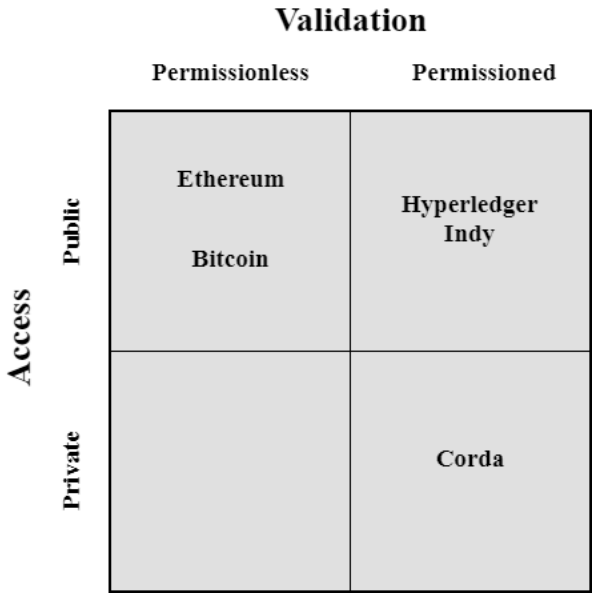

Table 1. Access - validation matrix

The public permissioned distributed ledger model is chosen for Indy since the global identity ledger needs high scalability, trusted governance, an identity that is accessible to all, and a network that has strong privacy (Sovrin 2018, 15,17). Due to these requirements, at this stage of technological development, the blockchain model is not a suitable ledger for this use-case. Indy ledger uses *Plenum* as a consensus-algorithm which is the implementation of RBFT (Redundant Byzantine fault tolerance). Plenum allows nodes to have a consensus of the occurred events. (Hyperledger, 2019f) In Sovrin's model, the nodes are run by trusted institutions, so-called "*Stewards*" (Sovrin 2019).

According to Sovrin (2018), the SSI network should have the scalability and performance of the domain name system (DNS). Therefore, Sovrin uses two fundamentally different kinds of nodes. Validator nodes are run by trusted Stewards and these nodes have the permission to accept transactions. Only trusted and validated participants can act as validator nodes. Examples of this kind of entity could be universities or other non-profit organizations which do not have a conflict of interest. Observer nodes cannot validate transactions and are only running "read-only" copies. A lower level of trust is required from these nodes, and these nodes are used only to process read requests. This solution is used due to the limitation of consensus protocols that cannot scale indefinitely, and only a limited number of validators can be accepted. (Sovrin 2018)

2.4 Identity and claims

A brief look related to the concept of issuing and verifying claims related to the identity is needed to interpret the main entities and terms in this process as well as to achieve a common language. There is no universal definition for identity, but it can be considered as who a person, organization or thing is by using a set of claims made by the identity holder regarding itself (Cameron 2005; Fearon 1999, 11-12). A claim is an assertation of ourselves (identity owner) which is used to tell who we are. Usually, different kinds of credentials are used to prove that our claims are true. A credential is typically a document that provides information related to the document owner's identity (e.g. passport, driving license). (Sovrin 2018, 4)

Figure 10 below shows on high-level the process of issuing, proofing, and verifying claims related to identity. In the simplest scenario, there are three different entities involved in this process: *issuer*, *owner* and *verifier* of the identity. The issuer is a trusted party which issues a proof in the form of credential for the owner of the identity. The proof can be also called as verifiable claim if the issued proof can be verified. If the claim cannot be verified it is not a verifiable claim or proof, only a claim. (Sovrin 2018, 6).

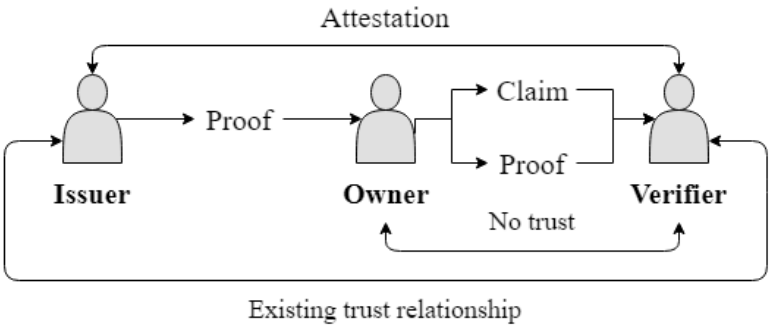

Figure 10. Concept of identity

The owner is the entity that owns and uses these issued proofs to verify own identity. The owner of the identity can be a person, organization, or thing. Verifier is the counterparty that wants to verify the owner's identity or aspects related to it (e.g. over 18, permission to drive, etc.). Usually, the verifier and the owner of the identity do not know each other, and thus they do not trust each other. (Sovrin 2018, 6).

The owner can make claims related to the owner's identity, but these claims are worthless if those claims cannot be verified. Therefore, the owner uses proofs that the verifier can trust, so-called verifiable claims. The verifier can only trust documents that are issued by an entity

that the verifier can trust. This means that the verifier and the issuer need to have an existing trust relationship between each other. Otherwise, the verifier cannot trust to the provided proofs. Usually, state agencies and financial institutions are widely trusted issuers and thus often act as trusted parties which the verifier can trust. The most reliable proof is an attestation from the issuer. An attestation is a proof where the issuer directly issues proof to the verifier. For example, if the verifier wants to ensure the validity of the identity owner's university diplomas the verifier could contact the university where the owner was graduated and thus get the proof directly from the trusted issuer without trusting the proof provided by the identity owner. (Sovrin 2018, 4-6).

2.4.1 Evolution of digital identities

According to Sovrin (2018) "*digital identity is one of the oldest and hardest problems on the Internet*". This is because the Internet was built without an identity layer, a standard way to identify different entities using it. The Internet's addressing system only identifies machines on the network, not the end-users, individuals behind the machines. Therefore, there is no standard way to verify online identities, and it is difficult to trust the proofs provided by the Internet since these proofs are very difficult to verify. (Sovrin 2018) According to Allen (2016), there can be seen various steps in the evolution of digital identities. The main steps can be seen in Figure 11 below.

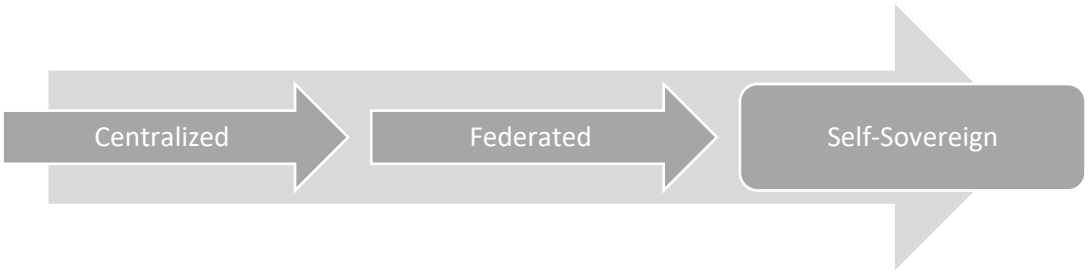

Figure 11. The evolution of digital identity

Centralized identity refers to an identity that is controlled by a single authority. This means that the identity is issued and controlled by a single central authority. There are various issues which arise due to the centralized approach. First of all, users are locked into a single authority that has the power to revoke a user's identity anytime and thus allocate the power from the identity holders to the centralized authorities. In addition to that, users need to

manage dozens of different digital credentials (e.g. passwords and usernames) since for every new connection, new digital credentials need to be created, which leaves users to manage separate credentials for each relationship. Unfortunately, centralized authorities are not always trustworthy. A centralized way of managing identities leads to a so-called "single point of failure" since identities are stored and managed within trusted parties or their service provider's database. (Sovrin 2018, 4, 7; Allen 2016) This makes these databases honeypots for hackers, and unfortunately, data breaches happen at times. The latest known example was the Equifax data breach which affected approximately 143-148 million individuals in the United States, or almost half of all the residents in the United States. (Federal Trade Commission 2019; McCrank and Finkle 2018)

The federated identity model allowed users to utilize the same identity on multiple sites and thus gave some portability for the identity compared to the centralized identity. This allowed users to sign in and log onto third-party platforms with existing identity. This simplifies the authentication process and reduces the number of usernames and passwords that the user needs to manage, thus improving the user experience. (Allen 2016) In the federated identity model, there is a trusted third party acting as an identity provider between the user and the service which federates the login to the service (Microsoft Azure 2017). Unfortunate this centralized the power even more since users are now even more dependent on the identity provider which acts as a third-party.

Finnish Trust Network (FTN) (former TUPAS) is a strong electric identification and digital signature framework in Finland supervised by the Finnish Transport and Communication Agency (TrafiCom 2019). FTN is based on the federated identity model (Nordseth, 2009, 12). In Finnish Trust Network, Finnish banks and telecommunication operators act as an identity provider for the end-users. End users can present their identity for service providers by using an identity broker which handles the authentication request between the service provider and the identity provider in the Finnish Trust Network. The identity holder can choose the identity provider that they want to use and authenticate themselves for the identity provider, which then verifies the identity. The end-user is redirected to the service provider by the identity broker after the identity authentication is successfully performed and the identification data from the identity provider is delivered to the service provider. (Idfy 2019; Pyöriä 2018; TrafiCom 2019) However, this leaves the end-user to be dependent on the

identity broker and the identity provider. In addition, this authentication procedure is limited to be used only in Finland and is not compatible with all internet services.

2.5 Self-sovereign digital identity

The evolution of digital identity is now on the edge of taking a step to the self-sovereign identity model. (Sovrin 2018, 2) The Internet was built without a way to know who you are connecting to (Cameron 2005). According to the Sovrin (2018), the coming evolution of the Internet will be a universal digital identity layer that allows all entities to have their own self-sovereign digital identity that is generated, owned and controlled by the entity itself. These aspects make it principally compatible with the European Union's GDPR-regulation and MyData principles proposed by the Finnish Ministry of Transport and Communications. (Sovrin 2018, 20, 22, 33, 38; Reed, Law and Hardman 2017) The aspect of an entirely user-controlled identity is the main fundamental difference to the current centralized and federated way of managing identities where the identity is issued, owned, and controlled by centralized entities. The definition for the SSI is adapted from W3C (2019) and is defined as "*an identity that is generated and controlled entirely by the user itself and it is not dependent on any third parties or intermediaries"*

Self-sovereign-identity can be breakdown into three different aspects. 1) The identity does not depend on any central authority and is only owned by the individual, organization, or a thing. This means that the owners of the identity have full control over the digital identity, and they do not need to rely on any third party to issue them an identifier to their use. 2) The individual fully controls the use of data related to the identity. Identity holders can choose whether they want to share their identity data or not since identity holders control their own data. 3) The identity is universal and should be usable everywhere. The identity is usable from different digital services to traditional offline services. (Hotti 2017; Sovrin 2018, 10, 13) Digital identity today is not fulfilling any of these three points which means that in theory, SSI could disrupt the way we manage our digital identities in the future. The full list of the properties of SSI can be seen from Table 2 below, adapted from Allen (2016).

1) Existence. Users must have an independent existence.
2) Control. Users must control their identities.
3) Access. Users must have access to their own data.
4) Transparency. Systems and algorithms must be transparent.
5) Persistence. Identities must be long-lived.
6) Portability. Information and services about identity must be transportable.
7) Interoperability. Identities should be as widely usable as possible.
8) Consent. Users must agree to the use of their identity.
9) Minimalization. Disclosure of claims must be minimized.
10) Protection. The rights of users must be protected.

Table 2. The properties of Self-Sovereign Identity

The concept of SSI would not be possible without the new distributed trust model that emerged with the blockchain and distributed ledger technology. In premise, DLT, as well as blockchain technology, can be both used as a platform for SSI, but as was seen in the technology overview these ledgers have different properties and trade-offs. Blockchain and DLT both solve the issue related to the centralized root of trust, and both can act as a decentralized self-service registry for public keys and decentralized identifiers that are needed to have a self-sovereign identity. (Sovrin 2018 9 – 10) It should be noted there are no self-sovereign digital identity systems in existence, which could support millions of users at the time of writing this thesis (2019).

2.5.1 Decentralized identifiers and objects

A decentralized identifier is a new type of globally unique identifier, for the self-sovereign digital identity. DIDs are a self-generated identification number for the user derived from the user's public key. DIDs are used to identify entities and are under the control of the user. DIDs are recorded on the distributed ledger, thus removing the need for any centralized authority. Since there is no central authority managing the identifier and the DID is produced by the user itself, it is a truly self-sovereign digital identifier. (W3C 2019; Sovrin 2018, 10-11; Reed 2017)

Generation of DID's is based on cryptography and randomness, and it is practically infeasible to generate the same DID key pair twice by different users, hence the uniqueness of the identifier. DIDs are registered and verified cryptographically. An example of a decentralized identifier generated by using Sovrin's method can be found in Table 3 below. (W3C 2019)

did:sov:3k9dg356wdcj5gf2k9bw8kfg7a

Table 3. Example of decentralized identifier

As can be seen from the Table 3 above, DID differ from traditional human memorable identifiers (e.g. Social security number). Sovrin uses "pairwise pseudonymous identifiers" which reduce the correlation of the identifier and the identity. This means that the identity data is separated from the identifier and that for every new relationship a new identifier can be created. (Sovrin 2018, 20-21)

In the Sovrin trust framework, it is possible to generate new DID for every new connection, hence it is possible to have thousands of different DID's controlled by a single entity. DIDs can be publicly disclosed and written on the identity ledger or privately exchanged between parties. It is advised to use new DID with every new entity since it increases the user's privacy. (Windley 2019; Sovrin 2018, 20-21) This is a major difference compared to traditional identity solutions where the same identifiers are used in various places. Phone number, social security number, and usernames are an example of identifiers which are often used in various places at the same time. This leaves users vulnerable to identity theft and increases the cost of thefts since the same credentials can be used in various occasions. (Sovrin 2018, 21)

It should be noted that DIDs are universal identifiers and are not tied to a specific ledger. DIDs can be used in all the ledgers that support them and for this reason, there are currently being developed multiple different methods for implementing DIDs which can be seen from Table 4. below. The different methods can all specify their methods related to DIDs and DDOs. For example, how to create, read, update and delete different operations on DDOs and DIDs on the different ledgers. Each method has its own DID prefix. (W3C 2019; Reed 2018)

Method	DID Prefix
Sovrin	did:sov:
Bitcoin Reference	did:btcr:
Ethereum uPort	did:uport
Veres One	did:v1:
IFPS	did:ipid:
Bloockstack	did:stack

Table 4. DID methods and prefixes

DID is a Uniform Resource Locator (URL) that point to a DID document. DID document (or DID Descriptor Object (DDO)) includes so-called service endpoints that make it possible to interact with the entity in a trustable and safe manner. (W3C 2019) DDO is stored on a distributed ledger along with the DIDs (Sovrin 2018, 10). According to Reed (2018), the primary elements of DDOs can be seen from Table 5 below.

DID (self-describing)
List of public keys (for the owner)
List of controlling DIDs (for key recovery)
List of service endpoints (for interaction)
Timestamps (for audit history)
Signature (for integrity(optional))

Table 5. DID Descriptor Object

Each DID with the use of DDO will give its users a lifetime encrypted private channel with the corresponding entity and over these encrypted channels entities can freely exchange verifiable credentials with each other. The owner of the DID can provide proof that the owner owns and controls that specific DID since it is derived from the public key and the owner owns the private key associated with the public key. (W3C 2019; Sovrin 2018, 10) The cryptography behind the DID is known as a public-key infrastructure (PKI) and the foundation of PKI can be traced back to the 1970s. However, since the DIDs reside on a public *distributed* ledger it could be argued that this architecture reminds more of a decentralized PKI (DPKI). DPKI refers to “decentralized key-value data stores” such as blockchain or DLT, and since the trust is decentralized, no single third party can manage the system as a whole. (Allen et al. 2015)

2.5.2 The process of issuing and verifying claims

Figure 12 below describes the process of how verifiable claims can be issued, presented, and verified by using self-sovereign identity. As an example, could be used the process of how a digital driving license could be issued in Finland in the future by following the principles of Reed (2018).

At the beginning of the process issuer and the owner of the identity needs to generate a public-private key pair for themselves. The private key is used to sign claims and the public key is used to generate decentralized identifiers and to verify the signed credentials. Therefore the issuer of driving licenses, Finnish Transport Safety Agency (TrafiCom) and the upcoming owner of digital driving license should both generate a public-private key pair for themselves. Involved entities can now generate their own decentralized identifiers from the public key. (Reed 2018)

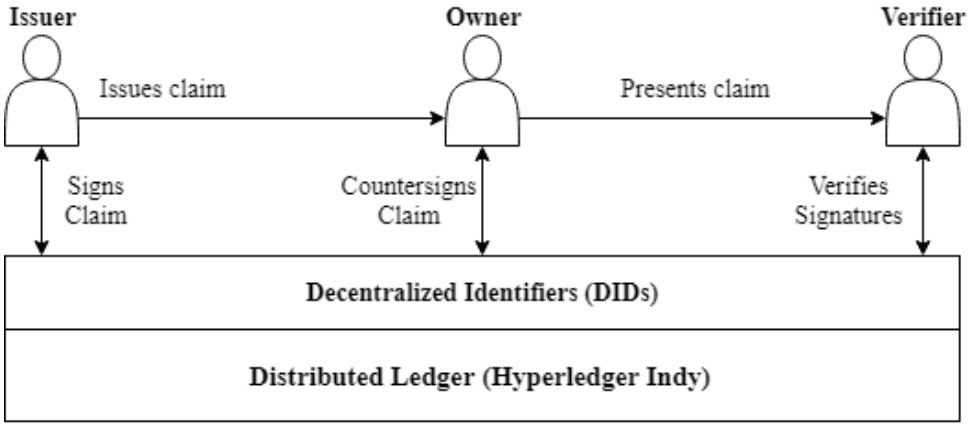

Figure 12. The complete process of issuing and verifying verifiable claims

It is advisable to generate a new DID for every new contact to preserve identity and reduce the correlation of identity. When both parties have generated the key-pair TrafiCom could issue a digital version of the driver's license to the owner and sign it by using its own private key. The owner can now countersign these claims by using his own private key. The digital driver's license can be stored on the owner's digital identity wallet in the mobile phone and when needed the owner can present this credential, for example, using a QR-code in the driving license. The driving license can be cryptographically verified when the owner wants to prove his identity by using the driving license as a credential. The verifier can scan that

credential and verify from the distributed ledger that the public keys and signatures are correct and that TrafiCom has actually issued that driving license to the owner. (Reed 2018)

Cryptographically it works since DID points to DDO which acts as a service-end point in between the identity holder and the verifier. DDO holds the public key of the identity holder and thus claims can be verified by decrypting them by using the DID holder's public-key. Verifier can verify the provided claims by using the issuer's public key. Verifier can choose whether to trust the verifiable claim provided by the issuer. (i.e. if the verifier can trust the issuer of the claim.) In this situation, the verifier and the issuer have already an existing trust relationship and thus verifier can trust the provided credential. (Reed 2018; Sovrin 2018,11; Reza, Nguyen and Aijun 2018)

3 LITERATURE REVIEW

In this chapter, a literature review is conducted to find previous relevant academic literature related to the field of this study. An effective literature review creates a strong foundation for advancing knowledge, and it forms the basis for empirical research, according to Webster & Watson (2002). This chapter begins by introducing the literature review methodology and then proceeds to the literature review itself.

Currently, there is an increasing amount of academic literature related to distributed ledger and blockchain technology. However, no evidence of DLT being applied to the founding process of a limited liability company priorly to this has been found. Therefore, this literature review is building an umbrella term discussion related to distributed ledger and self-sovereign identity to produce a complementary view of the research theme. However, the main focus is on self-sovereign identity since it is the key technology used in this study. A literature review related to the methodologies of this study is conducted as well.

This literature review is divided into two main sections, first, there is a literature review related to the subject of this study, DLT and SSI. Literature review related to the methodologies used in this thesis follows after the research subject to make this review extensive and to include necessary academic literature where the empirical part could be built on. There are five subsections related to the methodologies used in this study: case study, Monte Carlo-simulation, profitability analysis, consensus decision making, and interviews.

3.1 Methodology and source of literature

The methodology of this literature review is adapted from a three-step structured approach proposed by Webster & Watson (2002). The structured documentation collection process used in this study has the following steps:

1. *Defining keywords* and scan for major contributions in the leading journals.
2. *Scanning the search results*
3. *Backward tracking* by reviewing the citations used in the articles.

First step: At the beginning of the literature review, LUT Finna (2019) was selected as the main portal for searching relevant academic literature from the field of this study. LUT Finna

is an academic library that has access to over 100 different databases and thus offers an extensive and comprehensive view of the academic literature by itself (LUT Finna 2019). However, it should be noted that LUT Finna (2019) is only available for the students at LUT, but it searches databases that are publicly available. Google Scholar (2019) was chosen as a second research portal to acquire as much relevant literature as possible.

The search of source literature is limited by framing the publications from January 2008 to September 2019 to acquire as much relevant literature as possible. Bitcoin's white paper was released in 2008, and before that the concept of blockchain and DLT was unknown (Nakamoto 2008). Therefore, there are no relevant publications related to the field of this study before 2008. The main key-words and string targeted to relevant academic papers are formulated broadly to acquire enough relevant and interdisciplinary literature. First, the following search string combination was used: ("Distributed ledger" OR "Blockchain") AND ("Self-sovereign identity") search resulted in a total of 306 search results which only a dozen peer-to-peer reviewed articles. Thus, the search string was expanded to include the term "KYC" with the "Self-sovereign identity". The publishing year was set to begin from 2008 and English was chosen as a language. This resulted in a total of 3144 results with 106 peer-to-peer reviewed articles. Thus, the final search string combination used was: ("Distributed ledger" OR "Blockchain") AND ("Self-sovereign identity" OR "KYC") Search results were organized based on their relevance.

The second step: included scanning the research results and based on the titles, abstracts, key-words, introduction, and conclusion of the articles. Scanning of the search results unveiled that most of the search results were not relevant to the study, and 13 papers were chosen to include in the review whereas irrelevant articles were deducted from the review.

The third step: backward tracking was used for the effort to find articles related to the research theme that was not found by using the selected keywords. Backward tracking was conducted by reviewing articles related to the keyword and looking at references that had an important contribution to the paper or was in another way related to SSI that was not found by the search engine. Backward tracking produced one more article to the literature review and thus the total number of articles utilized in the literature review is 14. This same three-step structure procedure is applied to the literature review related to the methodology of this study as well.

3.2 Distributed ledger technology and self-sovereign identity

As was seen in the technology overview chapter, distributed ledger technology is a broad concept and there are no established terms in this field. There is a large number of academic studies related to DLT since it is such a large concept and can be applied in various industries. According to the literature review, neither DLT nor SSI has been applied in the founding process of a limited liability company, thus this review focuses only on SSI and KYC related academic literature.

Soltani, Trang Nquyen and An (2018) studied how SSI and DLT, more precisely Hyperledger Indy, could be used for making KYC processes more efficient. They identified that current KYC processes are typically slow, expensive for the company and are conducted offline. They also noted that current identity management models are built in a way that users are not in control of their identity data. Also, due to the centralized model to storage the identity data, the data is scattered across multiple identity providers, which are vulnerable to cyber-attacks. In their study, they introduced a KYC2 framework on how Hyperledger Indy and self-sovereign identity together could be applied to know your customer processes. Soltani et al. (2018) noted that while the KYC2 framework is decentralized it is still dependent on various trusted centralized entities such as governments and banks which perform the original identity proofing. They also emphasize the need for a common trust framework agreement that describes the decentralized governance policies in the Hyperledger Indy trust network to make it work for the long term. Finally, they stress the importance of deployment and operation of nodes in the network since there needs to be an incentive structure in place for network operators due to the expensive commitment of operating node. (Soltani et al. 2018)

Stokkink and Pouwelse (2018) studied on how blockchain-based self-sovereign identity could be deployed. They quoted the ten principles of Self-sovereign identity proposed by (Allen, 2016) and advanced it by adding that general claims should also be *provable* since otherwise, claims would not be worth anything. According to Stokkink and Pouwelse (2018) to full fill all 11 properties of self-sovereign identity, the claims should have the following properties: portability, interoperability, minimalization, and protection.

Parra Moyano and Ross (2017) proposed a distributed based KYC system where customers can securely share their KYC information with all the financial institutions that they would

like to work with. The main finding is that the DLT allows the cost of the KYC process to be distributed among the banks which work with the same customers. More precisely, this means that the KYC process can be accomplished in a single bank and this KYC information can be shared with all the banks which are used to by the same customer. According to Parra Moyano and Ross (2017), DLT act as a single "point of truth" and the main improved over the current system is that the KYC process needs to be carried out only once by banks for each customer which reduces the total cost for the jurisdiction. However, they address that DLT systems are still in their early stages and the privacy regarding the customer data should be thoroughly addressed.

Dunphy and Petitcolas (2018) took a look at identity management schemes on the blockchain and concluded that DLT is not a silver bullet solution for Identity Management (IdM) solutions. They nominated the two most significant hurdles for this "nascent research area" which are cryptographic key management and its effects on the user experience and tightening regulation of storing personal data. They especially mentioned General Data Protection Regulations (GDPR) which was enforced in 2018.

Der, Jähnichen, and Sürmeli (2017) took a look at SSI from the perspective of opportunities and challenges. According to their research SSI increases the freedom of identity owners and it could deteriorate the power of "Big Five" which is referring to Apple, Microsoft, Google, Amazon, and Facebook since they are services that a lot of people use and are in charge of managing digital identities for millions of users. According to the findings of Der et al. (2017), SSI could be very GDPR compatible since it empowers the users and gives individuals the highest control of their identity data and the possibility to select whether the users want to share data related to identity or not. SSI could also increase the strength of the European digital single market since it is transparent and thus remove the blockade of missing trust.

Coelho, Zuquete, and Gomes (2018) proposed a self-sovereign identity scheme, which is not using a public blockchain but a distributed ledger that is maintained by "regulation bodies" (RBs) and "service providers. (SPs)" Coelho et al. (2018) acknowledge that this kind of system requires trust between the users and trusted entities that maintain the ledger, and thus they generalize that: "The society, in general, trust on RBs to do proper supervision of their business sector and to keep a coherent blockchain among themselves." However, they do not disclose more specifically what could be specified under the term "RBs."

Gruner, Muhle, Gayvoronskaya, and Meinel (2018) studied how the current identity management could be improved with the use of blockchain technology and they propose a quantifiable trust model for blockchain-based identity management. Gruner et al. (2018) studied the trustworthiness of SSI based identity model by using directed graphs. Self-sovereign identity management requires a different trust model due to its decentralized nature. Gruner et al. (2018) underline two challenges that the SSI model faces. The security model of SSI is based on the pre-trusted group of digital identities which are the first identities in the network. Therefore, these identities act as an initial source of trust. This partly affects the decentralization and actually centralizes the trust to a certain extent. Malicious identities in this group can subvert the trust model since they act as pre-trusted members whereas new identities need to build their trust when joining the network. Therefore, pre-trusted identities need to be carefully selected into the network. The more there are pre-trusted entities, in the beginning, the better it is in premise since it distributes trust between various different entities and decreases the centralization. The second challenge which they underline is the nonexistence of a punishment process to penalize malicious act. There is no difference between malicious and trustworthy claims which can deteriorate the trust-model of SSI. The usage of verifiable claims should always lead to an increase in trust, not to decrease of trust.

Ferdous, Crowdhury, and Alassafi (2019) analyzed the existing definitions of self-sovereign identity and provided a formal definition of SSI by using a mathematical model. The relation between the user of the identity, identifier and partial identifier (attributes) as well as the (total) identity of a user was mathematically modeled. Ferdous et al. (2019) analyzed the existing definitions of SSI and proposed a list of properties that SSI should meet: existence, autonomy, ownership, access, single source, protection, availability, and persistence. These properties were used to compare existing SSI systems complemented with choosability, disclosure, consent, portability, interoperability, minimization, transparency, standard and cost where then compared between existing SSI systems. Ferdous et al. (2019) included uPort, Jolo, Sovrin, and Blockcerts into the comparison and used a table to visualize the results. Sovrin was seen as the most compatible with the chosen properties according to the results but Ferdous et al. (2019) acknowledged the incompleteness of the systems since none of the systems fulfilled all properties. Finally, Ferdous et al. (2019) proposed possible use-cases for SSI including registration, de-registration, authentication/authorization, identity provisioning, and service provisioning. These can be seen as components that are required

in the founding process of an LLC but in isolation cannot be used to digitalize the company founding process.

Haddoudi, Ech-Cherif, and Dafir (2019) analyzed and compared the following SSI management systems: uPort, Sovrin, and ShoCard. All of these systems had different advantages but Sovrin satisfied most of the proposed criteria. However, especially the user experience of Sovrin was criticized and users found it too hard to understand.

According to Takemiya and Vanieiev (2018), proofing the digital identity remotely is difficult to do, since the digital identity usually is not global, absolute to construct and the information shared with different parties varies. Takemiya and Vanieiev (2018) state that users should have full control over their identities and they should be able to share only the information which they would wish to share with different services. Takemiya and Vanieiev (2018) address the possibilities of blockchain and DLT technology as an enabler for self-sovereign digital identity due to the decentralized way to handle the public key infrastructure. Takemiya and Vanieiev (2018) present a proof of concept called “Sora identity system” which uses a mobile app that leverages DLT technology to provide a fully self-sovereign identity for its users. Sora Identity utilizes Hyperledger-Indy codebase and uses Plenum as a consensus algorithm.

Zhou, Li, and Zhao (2019) identified the increasing differentiation of digital identities, fragmentation, and centralization of identity information as the main issue related to the current digital identity. Abraham, Theurmann, and Kirchengast (2018) address the issues that traditional identity management systems suffer. The main issues are the reliance on a single centralized party and users' lack of control over their identity data according to Abraham et al. (2018).

Zhou et al. (2019) in their paper propose a self-sovereign identity framework named “EverSSDI”, build on top of Ethereum blockchain by using smart-contracts. Ever SSDI has two decentralized identity recovery schemas for self-sovereign identity. The first recovery method is based on social networking services (SNS) authorization and the other is by using Ethereum Oracles. Zhou et al. (2019) state that the SSI enables users to become the real owner of the identity instead of only a prover of the digital identity.

According to the KPMG (2018) report, the banking sector invests an excess of 25 billion US dollars on financial risk management. The majority of the cost is assigned to KYC

procedures. According to the KPMG (2018), the KYC services are extremely inefficient and up to 80 percent of the resources are spent on the customer information gathering and processing and only 20 percent to assessing and monitoring the gathered information. The largest value proposition of DLT in this process is the possibility to share the customer information between different organizations and thus the identification and verification for the customer can be performed only once per customer. However, this would need collaboration between regulators, service providers, and technology firms. DLT could change the KYC "know your customer" process into WAKOC "we already know our customer" process.

Academic studies overall recognize the limitations related to the current centralized identity management model. The main limitation is the user's lack of control over their identity data. (Abraham et al. 2018; Zhou et al. 2019; Parra Moyano 2017; Takemiya et al. 2018). The potential of blockchain or DLT based self-sovereign identity system was recognized in various studies. From the existing self-sovereign identity model Sovrin model was identified as the most promising and compatible SSI system. (Haddoudi et al. 2019; Ferdous et al. 2019) KYC processes were identified as a potential use-case for SSI and DLT in various papers (KPMG 2018; Parra Moyano et al. 2017; Soltani et al. 2018). Soltani et al. (2018) introduced a KYC2 framework which applied the same technologies used in Project Mercury and thus was the most relevant literature related to the Project Mercury.

3.3 Literature review on the methodologies

A literature review is conducted on the methodologies applied in this study to achieve a holistic view of the research process. This includes a review of a case study, Monte Carlo simulation, profitability analysis, consensus decision making, and interviews.

3.3.1 Case study as a research approach

A case study is a research method that studies one or a few cases in-depth and in detail within the context of the research subject. Usually, case studies cannot be generalized since there is no sample that represents a larger population. The potential advantage of a case study is to have a detailed description and analysis of an object of research and to make new

observations related to the phenomena. (Mills, Durepos and Wiebe 2010; Ridder 2017) Bent (2006) concludes that a case study is the most useful when trying to understand complex and unknown issues. According to Piekari, Welch and Paavilainen (2009) case study is the most popular qualitative research strategy. Yin (2013, 3-4) suggest to apply a case study when the main research questions are "how" or "why" questions and when the research question requires an extensive and "in-depth" description.

Case studies can be divided into six subcategories in which, illustrative case study represents one category. The primary aim of illustrative case studies is to describe and show-case the researched phenomenon. It is often used when the research subject is not well-known or studied, and the primary objective is to describe what is happening and why it is happening. An illustrative case study is the most useful when the target audience of the study is uninformed about the topic. Illustrative case studies should describe all the elements and aspects in a case. Description could involve entities involved in a case, process steps, location, goals, etc. In an illustrative case study, it is important to keep the language understandable for the target audience. The purpose of the illustrative case study is to increase the knowledge related to research subjects and provide a common language and terms for discussing the topic. (The U.S. Government Accountability Office 1990, 37 – 40)

Tziralis, Kirytopoulos, Rentizelas, and Tatsiopoulos (2009) introduced a holistic investment assessment method that is based on genetic algorithm optimization and simulation to ease the decision-making related to investments. Tziraliz et al. (2009) used an illustrative case study of two mutually exclusive investment scenarios to demonstrate the usage of their investment assessment method. An illustrative case study was used to illustrate in practice the usage of the proposed method.

Grigalunas, Chand, and Luo (2002) did an illustrative case study on investments related to container ports. According to the study, investments in container ports hold a lot of various risks. Grigalunas et al. (2002) used the Monte Carlo simulation and a dynamic discrete-event model to illustrate the methodology to assess this risk analysis.

A case study is the most useful when the main research questions are "how" or "why" questions and when the research question requires an extensive and "in-depth" description Yin (2013, 3-4). An illustrative case study is a subsection for case studies and it is used to describe and show-case the researched phenomenon. The purpose of the illustrative case

study is to increase the knowledge related to the research subject and provide a common language and terms for discussing the topic. (The U.S. Government Accountability Office 1990, 37 – 40)

3.3.2 Monte Carlo- simulation as an analyzing technique

Monte Carlo simulation method was developed by Stanislaw and Metropolis (1949) during the Manhattan Project to solve problems related to the building of nuclear fission weapons. Monte Carlo simulation has gained a lot of popularity since then, and it has been used for various applications in different industries.

In the field of business, a simulation-based approach is often used as a part of investment analysis, more specifically, in portfolio analysis (Guodong (2013). According to Guodong (2013) and Wei, Jian, and Jianglan (2011), one of the main advantages of the Monte Carlo simulation-based approach is a large number of scenarios for a wide range of possible future events. Also, since there are various different risk factors and different kinds of uncertainties, simulation-based methods can help to realize the degree of risk. The results of the simulation can be visualized by using actual distributions of the results which give a great deal of information. Wei et al. (2011) simulated NPV values 1000 times to achieve the result they wanted.

Daoyuan (2010) used a Monte Carlo simulation to address the risk related to investment. Microsoft Excel was used for the simulation, and NPV values were simulated. Simulated results were presented in the summary table without visualization. According to Daoyuan (2010), the number of simulations drastically affected simulation errors and the accuracy of the results. Smaller simulation errors indicate more accurate results. The simulation was conducted for three different investments A, B, and C three times for each with 100, 5000 and 10 000 simulations. Simulation errors decreased drastically when the number of simulations increased. This indicates that a higher number of simulations decrease the value of simulation errors and thus produce more accurate results. 10 000 simulations produced approximately 32 % smaller simulation error compared to the 5000 simulations. Daoyuan (2010) analyzed the simulation error by using the following equation:

$\frac{s}{\sqrt{n}}\ t_{\alpha/2}(n\ -\ 1)$ where α is confidence level and $t_{\alpha/2}$ (n − 1) is quantile.

Equation 1. Simulation error (Standard error of the mean)

A non-normal distribution increases the standard error of the mean and thus might result in a wrong interpretation of the data. The standard error of the mean is the most useful to analyze when the population is normally distributed or when deciding the number of iterations for non-normally distributed data. The standard error of the mean should decrease when the number of iterations is increased.

Platon and Constantinescu (2014) applied Monte Carlo simulation in risk analysis for an investment project. They evaluated the performance of environmental projects by using IRR and NPV values. Platon and Constantinescu (2014) address that by using the Monte Carlo method the distribution of all possible outcomes of an event is generated. They applied 1000 simulations in their study.

Wei, Jian, and Jianglan (2011) used a Monte Carlo simulation to analyze mining investment risk. According to Wei et al. (2011), the mining investment risk related to mining projects often cannot be accurately judged since there are too many influential risk factors that affect the profitability and risk of that investment. Thus, Wei et al. (2011) applied a Monte Carlo simulation to take into account various different risk scenarios. The result was analyzed with NPV distribution and they used 1000 iterations to acquire accurate results.

Uwe and Özgur (2015) did an economic risk analysis of decentralized renewable energy infrastructure by using Monte Carlo simulation. The results were analyzed with NPV distribution and using “numerously repeated runs (>1000)”.

Based on the literature review the results of the Monte Carlo simulation are mostly analyzed with NPV distributions and by using 1000 iterations. (Uwe et al. 2015; Wei et al. 2011; Platon et al. 2014) Statistical tests are rarely used with the simulation and only standard error of the mean was used by Dayoan (2010). 10 000 simulations produced significantly smaller standard errors of the mean than 100 or 5000 simulations (Dayoan, 2010). This indicates that there are benefits to be achieved with more iterations, especially with more complex simulations (high number of input values, broad distribution within the minimum and maximum values).

3.3.3 Profitability analysis in the academic literature

Profitable capital investments will increase the prosperity and growth of a company and larger in the economy. Investors need techniques to predict the profitability of a proposed investment. Investment evaluation techniques can be divided into five main categories: Net present value methods, rate of return methods, accounting methods, ratio methods, and payback methods. The most popular methods are net present value criterion methods, internal rate of return method, external rate of return method, return on investment method, benefit/cost ratio method, and payback period method. According to the surveys made to Fortune 500 companies no investment analysis was ever conducted without using either the internal rate of return method or the net present value criterion methods. (Remer and Nieto, 1995)

Net present value might be the single most used calculation methods to analyze the profitability of an investment. The NPV calculation method was formalized by Fischer (1907). The basic idea with net present value is simple, it is the difference between the present value of cash outflows and the present value of cash inflows over a period of time. (Gaspars-Wieloch, 2017)

IRR is especially useful when investment with different amounts of capital or lifespan is compared between each other. The higher the IRR of investment is, the more preferable the project is. Positive IRR indicates that the project is profitable. Generally, the project with the highest IRR should be considered (ceteris paribus). Projects with negative IRR should not be accepted. It should be noted that IRR itself does not tell the present value of the project, only the internal rate of it. Thus, it is useful to compare projects by using both IRR and NPV to get a complementary view. (Ikäheimo et al. 2011, 130; Gaspars-Wieloch, 2017)

Discounted payback period also accounts for the time value of money, but another alternative is to calculate it without using the discount rate. By taking account of the discount rate, inflation, risk and opportunity cost are better included in the calculation, thus it can be seen potentially as a more accurate way to calculate the payback period. However, the discounted payback period is strictly limited to the amount of time required to pay back the initial investment by using discounted net cash flows. After the payback period investment might experience sharp movements that are not taken into account in this calculation method. Therefore, the payback method might not be useful if there are wide variations of future cash

flows or when estimating the long-term profitability of an investment. (Ikäheimo et al. 2011, 130; Gaspars-Wieloch, 2017)

3.3.4 Consensus decision making in the academic literature

One benefit of working in a group is the improved accuracy of decision making, also known as the "wisdom of the crowds" -effect according to Cronin and Stumpe (2014). The improved accuracy is explained by a larger number of people which can contribute to the decision making, producing a larger information pool from which more accurate decisions can be drawn (Cronin and Stumpe, 2014). Choudhurym Shankar and Tiwari (2015) came to a similar conclusion and stress the importance of collective skill and knowledge of the group which is usually higher than individuals. Consensus decision-making modeling can be also used to prevent the group from splitting if there are different opinions between participants (Dyer, Ioannou, Morrell, Croft, Couzin, Waters, Krause, 2008). Academic literature indicates that larger groups usually outperform smaller groups both in animals and humans in decision making. Smaller groups can increase the accuracy of the decisions by increasing the number of experts or other informed individuals compared to larger groups. (Cronin and Stumpe, 2014)

There is a prominent amount of academic literature devoted to animal behavior when studying consensus decision making, and there is surprisingly little academic literature related to consensus decision making in investment analysis. (Cronin, 2015; Lee, Teichroeb, 2016; Sumpter, Krause, James, Couzin, Ward, 2008; Conradt, Roper, 2005) The accurate investment decisions are essential for the profitability of the firm and inaccurate decisions might result in a significant decrease in the profitability and increase of costs.

3.3.5 Interviews as a research method

Interviews are often used research data collection method and there is plenty of literature related to it. The search term "interview" in LUT Finna (2019) shows approximately 2.7 million search results.

An interview is a flexible method of data collection and is therefore suitable for a wide variety of research purposes. Interviews are one of the most widely used methods of data collection. Interviews can be used to collect both quantitative and qualitative information related to the object of the research. The interviews can be conducted by interviewing participants individually or by using a group interview. Interviews are often divided into three different formats: structured, semi-structured and unstructured interviews. The type and method chosen as an interview are always related to the objects of the research. (Hirsjärvi and Hurme 2001, 34, 43-42, 61-62)

Structured interviews have a predetermined set of questions that are usually not diverged during the interviews. There might be both fixed and open answers for the interview questions. Due to a simplistic and straightforward nature, a structured method is often used in quantitative research for collecting data for statistical analysis. (Eskola and Suoranta 2000, 86)

A semi-structured interview method has a set of predetermined question and additional questions might arise during the interviews. Semi-structured interviews enable the interviewer to ask additional questions and deviate from the original structure. Semi-structured interviews are especially useful when there is a need to pursue in-depth information related to the topic and simple questionnaire cannot be used due to the complexity of the theme. Semi-structured interviews are usually conducted for a relatively small number of responders due to resource intensity. An unstructured interview has no interview questions prepared and is thus the least reliable interview method since the collection of data is performed in an informal way. (Hirsjärvi and Hurme, 2001, 45-47; Eskola and Suoranta 2000, 86-87)

Interviews allow research to collect detailed information about the object of the research and it is one of the most used data collection methods (Hirsjärvi and Hurme 2001, 34). Interviews also make it possible to ask for clarification if there are issues related to the data during the process. However, on the other hand, interviews require relatively much time to organize and prepare for the interviews.

4 METHODOLOGY AND DATA FOR ILLUSTRATIVE CASE STUDY

The empirical part of this thesis consists of a qualitative and a quantitative part and is thus divided into two different chapters. Chapter six is a qualitative study, and it is based on the illustrative case study. Chapter seven is a quantitative study and is based on the investment analysis simulation. The research methods and the source of data for different parts are discussed in separate chapters. The data and methodology for investment analysis are presented in the following chapter five.

In this chapter, the research subject, Project Mercury, is presented as well as the research methodology and source of the data for the illustrative case study. The accurate selection and interpretation of research methods is an integral part of the study since it acts as a foundation for interpreting meaningful insights into the research phenomenon (Fisher 2010).

4.1 A generic description of the research subject

In this chapter, a generic description of the research subject, Project Mercury, is conducted. Project Mercury is a collaboration of organizations that developed a proof-of-concept of the DLT-based business network that enables, in theory, a fully digital company founding process. This business network was set up between authorities and companies which are currently needed to be part of the limited liability company founding process. The participants of the Project Mercury can be seen from Table 6. below. The description of entities is adapted from the Project Mercury (2018). The Project Mercury was initiated at the beginning of 2018 with workshops and published the proof of concept in March 2018. The results of the Project Mercury were seen promising in the case company and thus a Project Jupiter was established, which act as a continuum for Project Mercury. The aim of the Project Jupiter is to establish a decentralized shared ledger and transaction network for non-listed companies. This study focuses on Project Mercury, but since there is a strong linkage between these projects, Project Jupiter is included in the investment analysis as well as in chapter 7.6 where future impacts and applications of Project Mercury are discussed.

ENTITY	DESCRIPTION
Financial institution	A financial institution provides business services to both individuals and companies. The FIs role is to enable a good financial starting point by enabling financial services to companies and enabling easy financial transaction services. FIs offer services during the whole lifecycle of the company. It's also the FI responsibility to perform KYC
Trade Register Office	A trade register office maintains a trade register. The Trade Register is a public register that contains information on traders and businesses. The majority of businesses are limited liability companies and private traders. The register contains official details of businesses all over Finland.
Tax Administration	Tax administration is a public official that will record the registration information at the end of the process. It will also verify the line of business proposed by the founder of the company.
KYC Brokering service / Information broker	The information broker will provide KYC and credit rating services. It is the broker's job to verify the background of the stakeholders and provide any additional information services, like credit checks, to the process.

Table 6. Project Mercury involved organizations

The role of the thesis worker was to participate in meetings, observe and collect information about how the company's founding process can be digitalized with the use of distribute ledger technologies by using Project Mercury as a source for data. The assignment included conducting a literature review on the DLT-based projects and to illustrate how the company can be founded digitally based on DLT. The assignment also included conducting a profitability analysis on Project Mercury.

4.2 Data collection process

Project Mercury (2018) can be seen as an end application for DLT-based technology. Therefore, the research data collection process started in a logical order by first collecting data related to the protocol layer, distributed ledger technology. This data was then complemented with data related to the application layer – self-sovereign identity, which eventually together formed the technology overview related to both SSI and DLT-technology. This built the foundation for the empirical part and for advancing knowledge.

It should be noted that since no prior research has emanated related to DLT-based company founding process, high quality, primary data related to the research subject is only available

directly from the Project Mercury (2018). Therefore, data for the illustrative case study and simulation is completely and directly collected from Project Mercury (2018).

The data for the illustrative case study has been collected by participating in various Project Mercury workshops during the project and utilizing internally shared project material. Data collection process related to this case study started by first participating in various workshops. During the workshops, data were collected by observing, discussing, asking questions and taking notes. At the end of Project Mercury, internal data were shared with project participants which complemented the acquired data from the workshops. With the use of internally shared material, workshops, and discussion made during the workshops it was feasible to form the illustrative case study. Table 7 below presents the used data type, source, and description of the data.

Category	Type	Source	Description	Duration	Date	n
Case Study	Workshop	Project Mercury collaboration	Project Mercury workshop #3	210 minutes	1.3.2018	<10
Case Study	Workshop	Project Mercury collaboration	Project Mercury workshop #4	210 minutes	27.3.2018	<10
Case Study	Workshop	Project Mercury collaboration	Project Mercury workshop #5	120 minutes	16.4.2018	<10
Case Study	Workshop	Project Mercury collaboration	Project Mercury workshop #6	120 minutes	8.5.2018	<10
Case Study	Workshop	Project Mercury collaboration	Project Mercury briefing session	210 minutes	1.6.2018	<10
Case Study	Material	Project Mercury collaboration	Project Mercury workshop material	-	1.6.2018	-

Table 7. Data for illustrative case study

4.3 Illustrative case study as a research method

This case study examines how the founding process of a limited company can be digitized by using DLT technologies. Due to the novelty of DLT and SSI, and the fact that there is no

academic literature related to the use of DLT in the founding process of an LLC it was cogent to choose illustrative case study as the main research method.

The main objective of this case study is to illustrate and describe in-depth how the use of decentralized ledger technologies can transform the current limited liability company's founding process into a digital one. This can be done by answering the research questions presented in the introduction chapter.

The type of this case study is illustrative which utilizes descriptive techniques to elaborate the research subject – Project Mercury in this case. Illustrative case studies are often used to describe a phenomenon or subject which is not well known. This study describes the main entities, technologies, and processes involved in Project Mercury. An illustrative case study provides definitions and a common language so that it is possible to understand and discuss the research topic in a wider audience. The study can be used to inform an audience that was previously uninformed about the research topic. This ease the cap between experts within this field and people who are interested in the research topic. Due to the illustrative nature of this research, this paper could be used to narrow the information gap between decision-makers and technological experts. Illustrative case studies are often used in internal marketing to advance knowledge within the organization. (Hayes, Kyer, Weber, 2015)

5 METHODOLOGY AND DATA FOR INVESTMENT ANALYSIS

In this chapter, the methodology and source of data for the investment analysis part of this study are described and in chapter seven the results are presented. The investment analysis is conducted by utilizing the Monte Carlo-simulation method. The valuation method is based on the intrinsic valuation method and the project is valued based on the estimated cash flows, growth, and risks (Damodaran, 2014). These input-values for the simulation are achieved by interviewing experts within the Project Mercury and by using a consensus decision making modeling to achieve consensus related to the input-values between interviewees. The value of Project Mercury is the net present value of the discounted cash flows. However, to have a better view of the investment, internal rate of return, as well as a discounted payback period, is calculated for the project.

5.1 Data for Monte Carlo- simulation

The case company did not numerically evaluate the financial benefits of Project Mercury since the project is in its early stage and due to the difficultness to estimate the associated cashflows. Therefore, semi-structured interviews were used to get input-values for the simulation. Three participants were qualified for the interviews, all within the same case company since interviewees needed a very high level of understanding of the Project Mercury. The questions were structured into different groups depending on the theme. However, since the estimation of future values related to Project Mercury is challenging there was room left for open conversation. According to Eriksson & Kovalainen, (2008) a semi-structured interview type is the most beneficial when studying so-called “what” questions, while still maintaining flexibility during the interview. It is important to include flexibility when the research subject is still in the nascent stage and is a complex subject.

The input-values for simulation were estimated by using minimum, maximum and most likely values which formed a triangular distribution for all input-values. This allowed a better inclusion of risk and uncertainties to the estimation. Interviews were conducted by using Skype, and the interviews took in between 90 to 120 minutes. Notes were taken during the interview so that the answers could be recorded. When all three interviews were conducted,

a joint Skype was held where the interviewees could see other interviewees' answers. The quantitative research dataset can be seen from Table 8 below.

Category	Type	Source	Description	Duration	Date	n
Investment analysis simulation	Interview 1	Case company	Input values for simulation	120 minutes	14.1.2019	1
Investment analysis simulation	Interview 2 & 3	Case company	Input values for simulation	90 minutes	30.1.2019	2
Investment analysis simulation	Interview and consensus decision making	Case company	Input values for simulation and results	90 minutes	7.2.2019	2

Table 8. Data for investment analysis simulation

One triangular distribution could be used per input-value for the simulation, thus consensus decision-making modeling was chosen to achieve consensus among the interviewees. The final input values for the simulation are estimated by using consensus decision-making modeling. The consensus decision-making process started by introducing a proposal that was produced based on Project Mercury material, the amount of code produced, and the number of employees involved in the project. This acted as a foundation and starting structure for the interviews. Then three industry experts A, B, and C were interviewed, and this proposal was introduced during the interviews. Industry experts modified and complement the proposal based on their own views. When all interviews were conducted, a consensus proposal was made by using a weighted average of the interviewee's answers.

This consensus proposal was given to these industry experts for testing the consensus. The consensus proposal was accepted after a discussion and by slightly modifying some input-variables. The consensus decision-making model used in the process is presented in Figure 14 below. If there were no consensus after the consensus proposal, discussion related to the input-values is used, which could lead to an agreement with the consensus proposal or modification of input values. This process could be repeated until there is a consensus achieved between the participants. It should be noted that the input-values are not officially agreed by the case company and are only intended to use for this academic study.

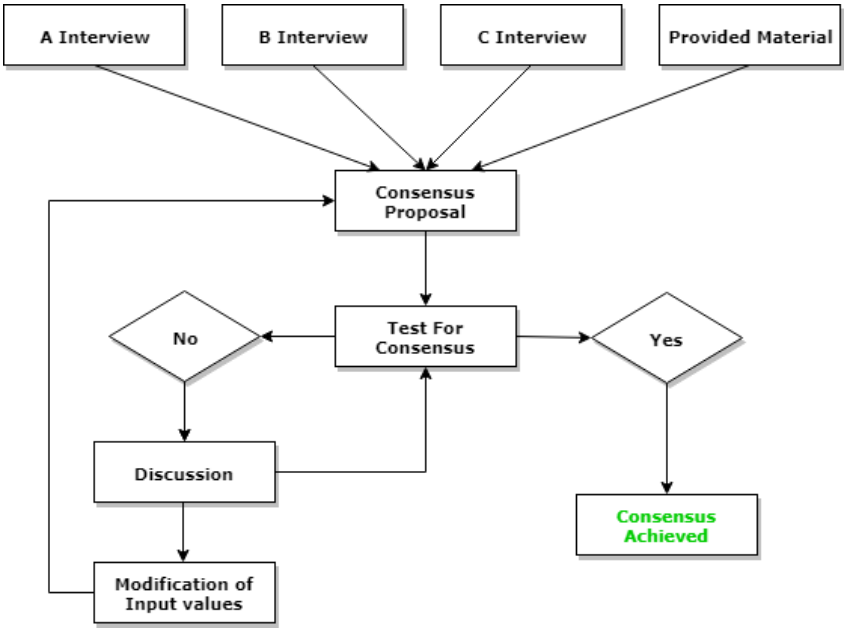

Figure 13. Consensus decision-making model

A total of 11 cashflow related input-values were selected for the simulation process. Uncertainty regarding the input-values of the simulation is included by applying triangular distribution. Investment analysis simulation is conducted by using a precautionary principle, which means that the possible profits were carefully assessed, and the risk and costs were stressed.

Table 9 and Table 10 presents the cashflow related input-values applied in the simulation. Values presented in the table are yearly values and the "Years" column indicates on which year(s) these variables are expected to generate revenues or costs. The investment is initiated at year 0, and the first cash inflows are estimated to be generated in year 3. Operational costs are estimated to increase at 3 % p.a. and revenues at 5 % p.a. Investment held time is estimated to be 25 years from time 0. Years 0, 1 and 2 are used for proof-of-concept, pilots and building for the commercial service, thus generating only initial investment costs.

Project Mercury and Project Jupiter are differentiated in the investment analysis simulation, but these projects do hold a similar cost structure in this estimation. The cost structure is estimated by using multipliers related to the initial proof of concept. The pilot project is estimated to cost 2 times (minimum) 3 times (expected) or 5 times (maximum) of the conducted proof- of concept. Similarly, the commercial service is estimated to cost 7 times (minimum), 10 times (expected) or 15 times (maximum) of the proof of concept. Operational

costs are estimated to be 20% (minimum), 25% (expected) or 30% (maximum) of the initial cost to build the commercial service.

Project Mercury is estimated to generate both cost savings as well as indirect revenues, whereas Project Jupiter is estimated to generate only revenues. Project Mercury is not expected to generate direct revenues, but the revenues are estimated to occur indirectly from the increased amount of both business and private customers due to the improved customer experience. Digital company founding and management process is offered only in banks which are part of the Project Mercury collaboration. Revenues of both projects are estimated to have a growth rate of five percent per annum. Cost savings are expected to occur, from more efficient processes, especially from the KYC processes, since company stakeholders are only needed to be identified once in the business network.

The major sources of costs are expected to occur first from the proof of concept, then from the pilot and finally from the fully functioning commercial service. These investments are made in stages and the feasibility to continue is evaluated after each stage. When the production-ready service is operating there are estimated to occur operating costs which are increasing three percent per annum. The exact triangular input-value distributions used in the simulation can be found in Tables 9 and 10. These tables present the cash flows associated with Project Mercury and Jupiter.

Project Mercury Revenues and Costs per Year	Minimum	Expected	Maximum	Years
Indirect revenues from new customers (5% increase p.a.)	100 000,00 €	150 000,00 €	500 000,00 €	3 - 25
Cost savings from more efficient processes	30 000,00 €	45 000,00 €	150 000,00 €	3 - 25
Proof of concept	-50 000,00 €	-60 000,00 €	-100 000,00 €	0
Pilot	-100 000,00 €	-180 000,00 €	-500 000,00 €	1
Commercial service	-350 000,00 €	-600 000,00 €	-1 500 000,00 €	2
Operational cost (3% increase p.a.)	-120 000,00 €	-150 000,00 €	-180 000,00 €	3 - 25

Table 9. Project Mercury Revenues and Costs

Project Jupiter Revenues and Costs per Year	Minimum	Expected	Maximum	Years
Tokenization of unlisted shares (5% increase p.a.)	100 000,00 €	150 000,00 €	500 000,00 €	3 - 25
Proof of concept	-50 000,00 €	-60 000,00 €	-100 000,00 €	0
Pilot	-100 000,00 €	-180 000,00 €	-500 000,00 €	1
Commercial service	-350 000,00 €	-600 000,00 €	-1 500 000,00 €	2
Operational cost (3% increase p.a.)	-120 000,00 €	-150 000,00 €	-180 000,00 €	3 - 25

Table 10. Project Jupiter Revenues and Costs

The discount rate is used to adjust the risk related to the investment. The real discount rate used in this investment analysis simulation is 15.3 percent. The real discount rate is calculated from the nominal discount rate and inflation. The nominal discount rate is

estimated at 17 percent whereas the inflation is estimated at 1.5 percent which results in the real discount rate of 15.3 percent. The equation used to calculate the real discount rate can be seen below in equation 2.

$$i = \frac{i' - f}{1 + f}$$

i = real discount rate

i' = nominal discount rate

f = expected inflation

Equation 2. Real discount rate

The nominal discount rate is derived from the risk-free rate and total risk premium for the investment. The risk-free rate used in the analysis is the Germany 10 years government bonds with a yield of -0.5% (Bloomber, 2019). The total risk premium for the investment is estimated at 17.5 percent. The risk premium is estimated by using the weighted average cost of capital + the risk premium of the project. The weighted average cost of capital is estimated at 4.5 percent using the banking industry average in the EU area. (Damodaran, 2019). The project risk premium is estimated at 13 percent. The usage of high real discount rate and project risk premium, during the yield of a negative risk-free rate, emphasize the precautionary principle (Ikäheimo, Laitinen, Laitinen and Puttonen 2011, 131-132). The values used in the analysis can be seen below in Table 11.

Discount rate	**Estimated values**
The real discount rate utilized in the analysis	15.3 %
Nominal discount rate	17 %
Inflation	1.5 %
Risk-free rate	-0.5 %
Total risk premium for the investment (a + b)	17.5 %
(a) The weighted average cost of capital	4.5 %
(b) Project risk premium	13 %

Table 11. Derivation of the discount rate

5.2 Monte Carlo- simulation

Monte Carlo simulation is conducted with Excel-spreadsheet and the simulation includes 10 000 iterations to maximize the reliability of value distributions. After each run, the NPV, IRR and DPP values are recorded in Excel. The recorded values are automatically collected to summary statistics and visualized by using net present value, discounted payback period and internal rate of return distributions in the results chapter.

For each input-value, there is a minimum, most likely, and maximum values estimated. Excel RAND-function is used to randomly fetch values from the triangular distribution. Equation three below presents the triangular distribution used in the study.

$$f(x) = \begin{cases} 0 & x < a \\ \dfrac{2(x-a)}{(b-a)(c-a)} & a \le x \le c \\ \dfrac{2}{b-a} & x = c \\ \dfrac{2(b-x)}{(b-a)(b-c)} & c < x \le b \\ 0 & x > b \end{cases}$$

Equation 3. The equation for the triangular distribution

"A" is used as a minimum value, "c" as most likely and "b" as a maximum value. Figure 14. A probability density function below visualizes the triangular probability distribution used in this study. The probability density function is dependent on the estimated range of different input-values. (Kotz and Van Dorp 2004)

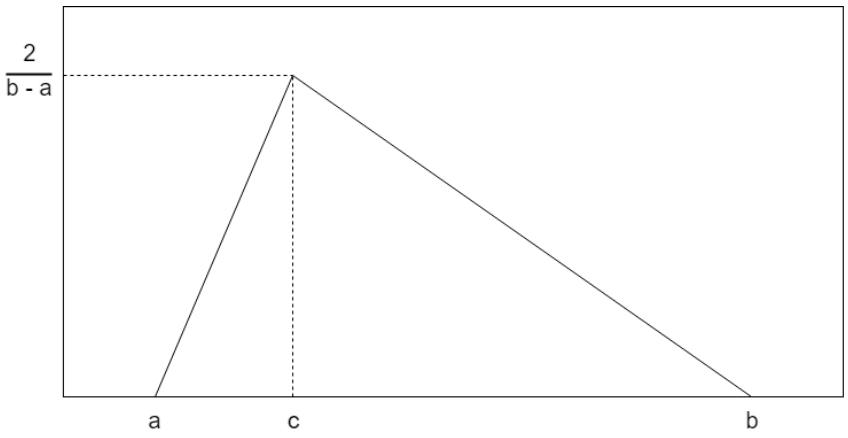

Figure 14. Probability density function

The triangular distribution is applied separately for all the estimated input-values seen in Tables 9 and 10. Triangular distribution differs between different input-values based on values given for “a”, “b”, and “c”.

5.2.1 Profitability indicators

The net present value, discounted payback period, and internal rate of return methods are used as calculation methods to estimate the profitability of Project Mercury for the case company. Various different calculation methods should be used when calculating the profitability of investment to produce a complementary view. The formula used to calculate the NPV is presented in equation four.

$$\mathrm{NPV} = \sum_{\mathrm{t=0}}^{\mathrm{T}} \frac{\mathrm{CF_t}}{(1+\mathrm{r})^{\mathrm{t}}} - \mathrm{C_0}$$

$$CF_t = Net\ cash\ flow\ during\ a\ single\ period\ t$$

$$r = Discount\ rate$$

$$t = Number\ of\ time\ periods$$

$$C_0 = Initial\ investment$$

Equation 4. Net present value

Net present value is a calculation method used to find the present value of estimated future cash flows. NPV takes into account the time value of money and thus can be used to compare different investment alternatives. Net present value rule dictates that only investments with positive net present values should be considered since positive NPV indicates that the investment will be profitable when future net cash flows are discounted to the present time. The discount rate is used in the NPV formula to take account of the inflation, risk and opportunity cost of an investment. The discount rate can be determined by comparing the riskiness of a project to other projects as well as accounting the cost of financing the project. The initial cost of an investment is deducted from the discounted cash flows which result in the net present value of an investment. Investment which results in the highest NPV should be chosen, if multiple different investments are compared. (Ikäheimo et al. 2011, 129-130; Gaspars-Wieloch, 2017)

NPV formula is highly dependent on the discount rate used since it has an essential effect on the profitability of an investment. NPV method with a high discount rate favors investment projects which can generate positive net cash flows from the beginning. A project with overall higher positive cash flows can get lower NPV values than a project with overall lower positive cash flows. This situation can occur if the used discount rate is high and positive net cashflows are expected to results farther away in the future than in a project with overall lower cash flows. Therefore, the cash flow distribution affects the net present value of the project. Even a relatively small change in the discount rate can make the difference between the positive or negative net present value for investment if the cash flows are occurring in the distance. Therefore, it is important to ponder which discount rate to use with the NPV method. NPV method measures the profitability of the project with absolute values. Thus, the size of the project affects the net present values and relatively more profitable projects might be rejected. (Ikäheimo et al. 2011, 130; Gaspars-Wieloch, 2017)

The internal rate of return is similar to net present value except that IRR is the discount rate where the net present value of an investment is zero and thus it is a relative measure. Internal rate of return can be used to complement the resulted achieved from the NPV method or to be used individually. The internal rate of return method ranks the projects based on their internal rate of return, thus projects with higher net present values might be rejected. (Ikäheimo et al. 2011, 130; Gaspars-Wieloch, 2017) The formula used to calculate the internal rate of return is presented in equation five.

$$\mathrm{IRR} = \sum_{t=0}^{T} \frac{\mathrm{CF_t}}{(1+\mathrm{r})^t} - \mathrm{C_0} = 0$$

$CF_t = Net\ cash\ flow\ during\ a\ single\ period\ t$

$r = Internal\ discount\ rate\ when\ the\ return\ is\ 0$

$t = Number\ of\ time\ periods$

$C_0 = Initial\ investment$

Equation 5. Internal rate of return

The discounted payback method can be used to calculate how long it takes for the project to pay back the original investment. Instead of using the sum of discounted future cash flows, DPP returns the time that it takes the investment to pay back the initial investment. The

discounted payback period recognizes the time value of the money and thus provides more accurate results. The project with the shortest payback period should be accepted. (Ikäheimo et al. 2011, 128)The formula used to calculate the DPP can be seen in equation six.

$$\mathrm{DPP} = \sum_{t=0}^{T} \frac{\mathrm{CF_t}}{(1+\mathrm{r})^t} \equiv \sum_{t=0}^{T} \frac{\mathrm{C_t}}{(1+\mathrm{r})^t} \equiv \mathrm{C_0}$$

$CF_t = Net\ cash\ flow\ during\ a\ single\ period\ t$

$r = Discount\ rate$

$t = Number\ of\ time\ periods$

$C_0 = Initial\ investment$

Equation 6. Discounted payback period

6 ILLUSTRATIVE CASE STUDY: DIGITALIZING THE FOUNDING PROCESS OF A LIMITED LIABILITY COMPANY

The empirical part of this thesis consists of two main parts. In this chapter, the illustrative case study is conducted to illustrate and provide insight into how the process of creating an LLC could be digitalized by using DLT technologies. This illustrative case study begins by first introducing a Corda and Indy-based business network and then step-by-step describes the processes of how a limited liability company can be founded digitally by applying distributed ledger technologies. This illustrative case study is based on Project Mercury (2018), and the data for this empirical part is presented in Table 7.

6.1 Corda and Indy-based business network

Project Mercury used Corda as a distributed ledger for recording, managing, and automating legal agreements between business partners and, thus, it acted as a backbone for the network between different entities. Hyperledger Indy is used as a distributed ledger for managing digital identities for companies and for exchanging verifiable claims related to identity. Indy is used for identity purposes only, all other information related to sharing and agreement handling is conducted by using the Corda network. Two different ledgers were used since the requirements for identity, and the managing of agreements are very different. The use of these specific ledgers was discussed in the technology overview.

Figure 15. below represents the overview of the relationships and interactions between the main actors in this new way for founding an LLC digitally. The process involves a co-operation of multiple organizations and stakeholders. Organizations involved in Project Mercury created a network between each other to facilitate the founding process of the company. Project Mercury participants were able to share information with each other in a secure way and practically in real-time. All involved organizations; financial institutions, tax administration, trade register, and information broker were running both Corda and Indy nodes. This makes the network more decentralized, and parties can directly verify and validate the transactions without trusting to intermediaries. As concluded before Corda was

used for shared business logic and Indy for SSI. Company stakeholders which are involved in the founding process used the user interface provided by the involved financial institutions.

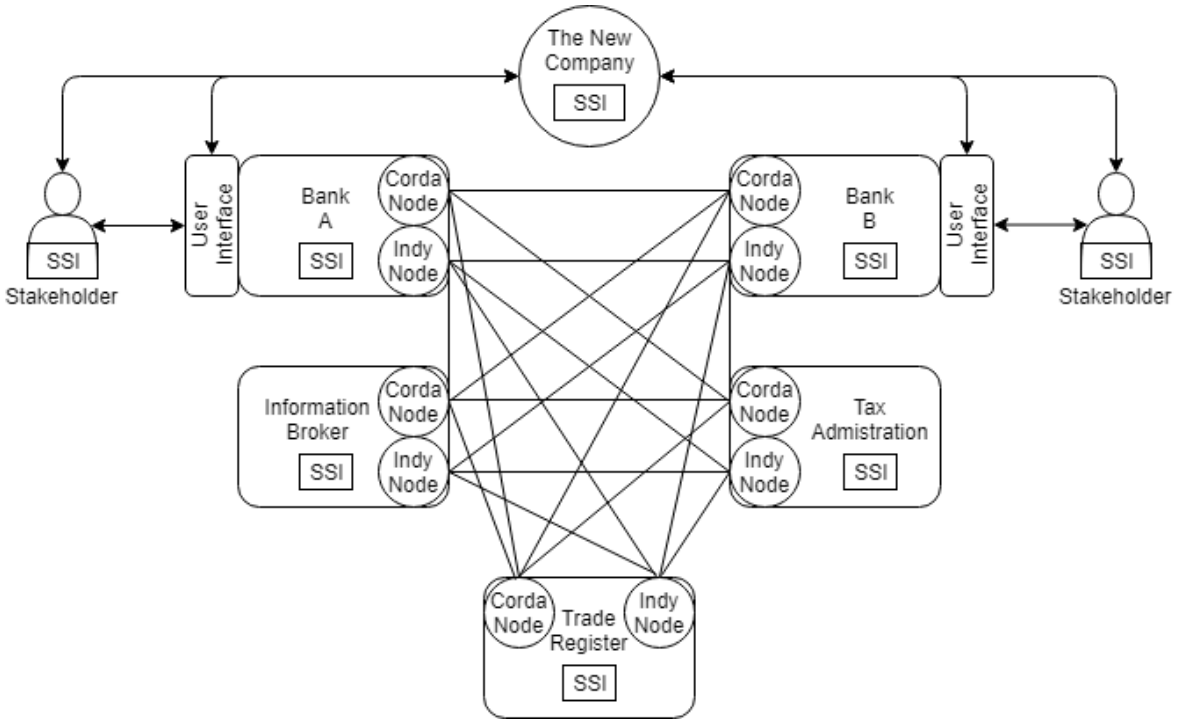

Figure 15. DLT based business network

When the network is initiated, and entities are running Indy nodes, globally available digital identity – self-sovereign identity can be created for the organizations in the network. Organizations involved in the Project Mercury need to create their own SSI before they can issue identities for company stakeholders and for the company itself. The process of creating, issuing and verifying SSI was reviewed in chapter 2.5.2 - technology overview. A similar process is applied when the organizations generate digital identities for themselves and later for the company stakeholders and for the limited liability company.

Table 9 represents the process steps that are used to found an LLC digitally. The preliminary requirements require that there is a DLT-based business network-enabled, as shown in Figure 16. This Corda based network is used for recording, managing and automating legal agreements between business partners and an Indy-based identity network is used for managing digital identities and for exchanging verifiable claims related to identity. The digitalized founding process is illustrated in the following chapters.

Process steps	Process step	Digitalized company founding process
Step 0. Preliminary requirements	0.1	Network participants run Corda and Hyperledger Indy nodes
	0.2	SSI is created for all involved organizations
The new LLC founding process:		
Come with a business idea		
Step 1. Initiate company draft	1.1	Creation of SSI
	1.2	Interacting with SSI
	1.3	Company founding documents and preliminary KYC
Step 2. Sign the founding document	2	Digital founding document signing with DIDs
Step 3. Assign representation rights	3	Representation rights are assigned for chosen stakeholders
Step 4. Approve transactions	4.1	Shareholder authorization to debit equity
	4.2	Full KYC check
	4.3	Create a bank account and debit equity from shareholders
Step 5. Review documents	5	Verification and registration
Business-ready limited liability company		

Table 12. DLT-based digital LLC founding process steps

6.1.1 Creation of SSI

The company founding process starts, naturally, by first coming with a business idea or with a need to found a limited liability company. When the business idea is clear, the founder needs to choose a financial institution that supports the digitalized company founding process. First, the founder will go through a KYC process by the corresponding financial institution if the person is a new customer. The authentication process can be unique for each financial institution, but it must be compliant with the Finnish Trust Network regulations and guidelines supervised by TrafiCom.

After the initial authentication process is completed by the financial institution, the process of creating SSI and DID for the stakeholders can begin. There are two main different ways

of how the DID can be created for the company stakeholders. The financial institution can act as a trust anchor and create and store the DID and the associated public/private key pair for the individual and thus acts as a kind of custody service for the individual. However, if the financial institution stores the private key, it can be argued that it is no longer a valid self-sovereign identity anymore since the user of the identity is not managing the cryptographic keys. Therefore, the identity holder would be depended on the financial institution.

The identity holder itself can also create the DID for his/herself by using an identity wallet[2] from the identity holders' own end device. This end device could be a mobile phone, and the cryptographic keys could be stored on phones secure enclave. This way, the identity is truly self-sovereign since the user is in control of the cryptographic keys. However, the secure storing of the keys is now on the user's responsibility. If the cryptographic private key(s) associated with identity is lost or stolen, users' identity is compromised. There are various different identity recovery models suggested such as social recovery, but currently, there is no de facto recovery mechanism in use. The secure cryptographic key management is an essential part of implementing a self-sovereign identity model successfully but is not in the scope of this thesis.

The newly created DID is used as a pseudonym identifier for privacy-preserving digital interactions whenever there is a need to represent identity or credentials. DID enable secure digital connection to share verifiable information with other DIDs. DIDs are used for "identification, authentication, digital signatures, verifiable claims, and other identity-related activities" in the forming process of an LLC (Project Mercury 2018). DIDs are not depended on the financial institution. It is universal, and all Sovrin DID holders are able to interact with each other. Therefore, each individual can choose their financial institution, which they want to use for generating DID for themselves (In case the financial institution acts as a custodian). However, this can be only done on financial institutions which are part of the same Indy network. DID is not usable by itself; it also needs a DID document (DDO) for the secure interaction. DDO holds the identity holder's public key and other key components that were presented in chapter 2.5.1 to have a secure digital interaction. The DID, as well as DDO, will be publicly disclosed to the Indy ledger.

---

[2] SSI identity wallets are not available for the public use since the Sovrin's SSI model is not finalized

On the second step, the financial institution which completed the KYC check will issue foundational claims for the company stakeholders so that the company stakeholders can present their identity by providing cryptographically verifiable proof to the verifier. The verifier usually has an existing trust relationship with the financial institution and thus can trust to the verifiable claim provided by the company stakeholder.

The newly created DID and DDO will be sent (by the bank or the identity holder, depending on the founding process) to the nodes running the Indy ledger which will reach consensus about the state of the ledger and include the DID and DDO onto the ledger. Indy is a shared ledger and owned by "nobody" and thus a single Steward (node operator) cannot censorship neither the DDO or DID. Thus, the attributes related to the identity that is controlled by the user, not a third party.

To make the SSI model complete, there needs to be Indy agents[3] that store the corresponding cryptographic key pair in the encrypted database. This database can be for example in the identity holder's mobile phone's secure enclave, and biometric access is needed for accessing the cryptographic keys, and thus, in premise, only the identity holder has access to the keys.

6.1.2 Interacting with SSI

In order to interact and share verifiable claims (e.g. proofs) one of the identity holders need to share their DID with each other, which can be used for deriving the corresponding DDO from the Indy Ledger. DDO contains service endpoint, which makes it possible for parties to connect with each other and change verifiable claims. Connecting party's agent sends a connection request to another identity holder. The other identity holder agent receives the connection request from the connecting party, and the connected identity holder can choose whether it wants to accept or decline the request. If the identity holder wants to accept the connection request, they have now formed a secure connection with each other to exchange verifiable claims with each other. It should be noted that the connection request only forms the connection but does not yet prove the identity holder's identity. Identity holders' Indy

[3] In computer science, "agent" is a piece of software which is used by parties wanting to act in the Indy network. The Agent software handles the verifications and signatures among other things.

agents are used to exchange DID's which then can be used to prove that the identity holder controls the private key which is used for signing verifiable claims.

The identity verification process starts with the identity proof request. The party that would like to verify the credentials or identity makes a proof request. The proof request schema is dependent on the context and the needs of the verifier. Therefore, different kinds of requests can be made, and the requester can choose whether it accepts the verifiable claims provided by the identity holder or if more verifiable claims are needed.

After the identity holder has received the proof request, it can now represent the verifiable credentials as a proof for the verifier based on the requirements received from the requester. The identity holder should construct the verifiable claim based on the requirements of the verifier. Financial institution issued the foundational claim for the identity holder and the identity holder can now use that claim for proofing attributes related to the owner's identity. Identity holder's financial institution digitally signed the issued claim, and thus the verifier can now verify the signatures from the DDO which is stored on the Indy identity ledger. When the identity holder has constructed the proof, it can be shown to the requester. The requester can now digitally verify it by using cryptography as explained above and verify the claims provided by the identity holder. Verifier, however, has still the possibility to choose whether it wants to trust the issuer. However, since the issuer is a well known financial institution in Finland, and the verifier has an existing trust relationship with the issuer, the proof can be accepted.

6.1.3 Company founding documents and preliminary KYC

When all involved entities have SSI, the company founding process can be started by the founder. The founding process can be initiated in the FI's web service which the founder is using. The founder can choose to start a new LLC from the main menu after the login to the web service. The company can be founded digitally only in FIs that are part of the Corda- and Indy-based business network.

The first step involves filling the company founding documents by the founder. Founding documents can be seen as the main document which describes all the essential information related to the soon to be founded LLC. This includes describing the name of the company, shareholders, business address, type of business, share capital, board members, and other

vital business information. The information requested in this step is similar to the information that should be provided to the trade registry office's Y1 document used in Finland. When the founder has created and filled the founding documents, and all involved stakeholders are nominated, there will be a preliminary KYC before the founder can sign the founding document digitally and share it to other stakeholders for verification and signatures.

The purpose of the preliminary KYC is to validate at the beginning of the process that there are no major issues with the company founding application. KYC is an obligatory requirement made for financial institutions to ensure adequate knowledge of their clients. According to the Finnish Law, stakeholders involved in the company creation should be audited.

Information related to the company is sent to the KYC service broker for auditing. KYC service broker validates the information related to the company, for example, if the company name is allowed to use, there is no ban on business operations, stakeholders are not underaged and if any of the stakeholders are not under guardianship. During the preliminary KYC, also a credit rating estimation for the company is established based on the business line of the company, it's key personal, and KYC brokering service's own internal process. When the KYC process is completed there will be a report created with success and failures for each section.

If for some reason there are issues detected in some section(s) the process cannot be continued until the changes are made for section(s) which did not pass the KYC check. These changes could be related to the name of the company if there are conflicting names, or by changing key personnel. The process can be continued when changes are made to the section(s) which did not pass the KYC check. When the preliminary KYC is completed, the founding process can be continued.

When the KYC check has been successfully completed the founding documents are created. This also creates a draft version of the digital identity for the company. However, the company is not registered in any registry yet, only a draft of it for shareholders to see the draft and verify it. Stakeholders can still choose whether they want to sign the company founding documents or suggest changes to it. When stakeholders have verified the draft, they can approve it by using digital signatures in the FI's service which they are using.

The founder can choose the stakeholders from contacts which the founder had connected before or during the founding process. Other stakeholders provided their DID, name and personal identifier (to differentiate persons with the same name) as a verifiable credential for the founder. DIDs are used to refer to the specific stakeholder and in premise, no other information is needed. However, the name and personal identifier ease the use of DIDs.

The founding documents are shared with stakeholders by using Corda based business network. Unlike in public blockchains, the data is only shared with stakeholders, not to anyone else participating in the network. It should be noted that by using SSI the shareholders, CEO and board members could come basically from any country or any FI as long as they are customers of the FI which is part of the Corda- and Indy-based business network.

6.1.4 Digital document signing with DIDs

This chapter introduces how the company founding documents can be digitally signed by shareholders using DIDs and distributed ledger technology. The document signing could be conducted anywhere from the world and without even having a Finnish national identity. The introduced digital document signing method can be used principally for any type of document.

When the company founding document is created and preliminary KYC completed stakeholders can review the founding documents. The stakeholders of the upcoming company will receive a notification from their FI’s service that the company founding documents are available for review. When the stakeholders sign in to their FI service, they are able to see the founding documents and that the founder has already signed the documents. Stakeholders are able to review the documents, and they can either accept the documents and digitally sign them, decline or propose changes if it does not satisfy the stakeholder. If there are changes to be made, the stakeholder can propose changes and highlight the changes by commenting on them. Change proposal is then sent to all shareholders in the network, and when all the necessary changes are finalized, the founding documents are shared with the involved stakeholders for review.

When stakeholders are satisfied with the founding documents, they can digitally sign it in the FI's service by using SSI. These digital signatures are verified cryptographically and

shared almost in real-time to the involved stakeholders. This same process is repeated to other stakeholders as well. Signed documents and signatures are stored on individuals' own personal vault in the bank's custody service.

Figure 16. Shows the process of how the founding documents can be signed digitally by using DLT and DIDs. The process starts by first applying a hashing function to the founding documents. When the documents are hashed, the identity holder can sign it with his/her private key. Hashed and signed founding documents are stored on the distributed ledger, which makes it principally impossible to counterfeit the founding documents.

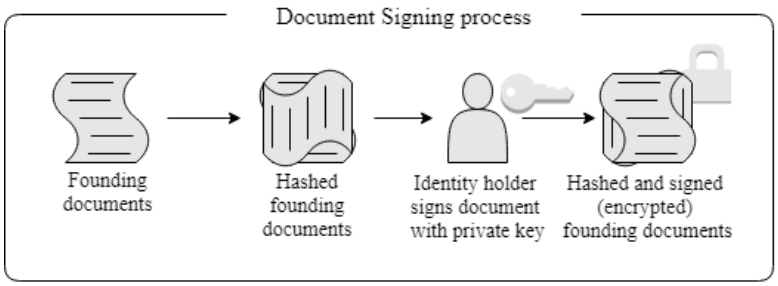

Figure 16. Document signing process

When the signatures and the founding document should be verified, reverse processes is applied as can be seen from Figure 17.

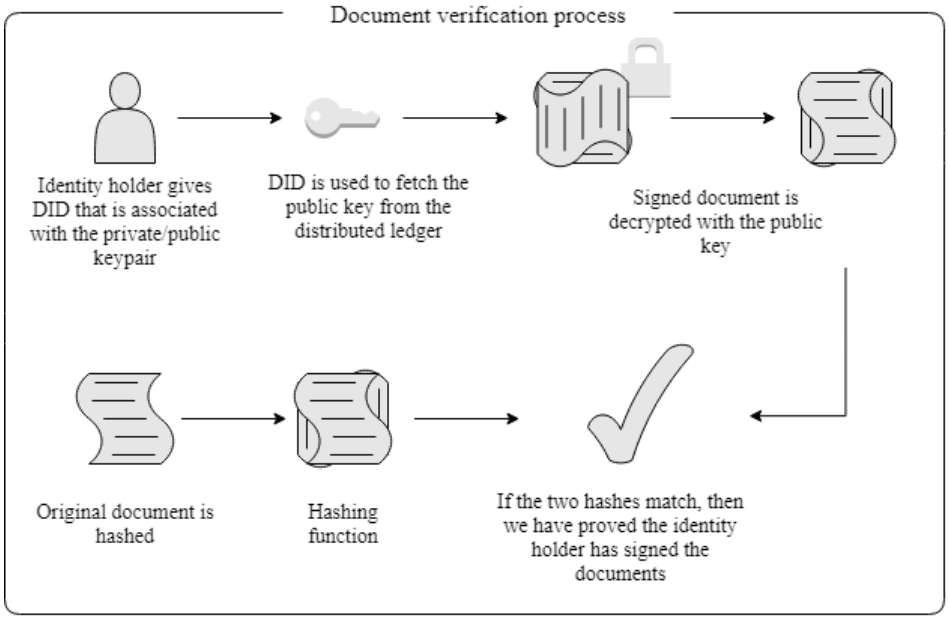

Figure 17. Document verification process

The document verification process begins by receiving the identity holder's DID, which is associated with the public-private key pair used to sign the founding document. DID is then

used to fetch the public key from the DDO document from the distributed ledger. The public key can be used to decrypt the encrypted founding documents. The original founding document which should be verified can be then hashed with the same hashing function used in the beginning and the hashes can be compared with each other. If the hashes match, we can prove that the identity holder has signed the document. However, if there is even a minor difference between the hashes, we can confirm that the identity holder did not sign the document or the document is different.

When all shareholders have verified and signed the founding documents, there will be automatically created a new DID for the company by the FI. However, this DID is not yet written to the Indy ledger and the public key is not yet made public. This is due to the fact that the company is still in the founding stage and does not have any legal status.

6.1.5 Representation rights for stakeholders

When all of the stakeholders have signed the founding documents, the founder can continue the founding process. The next and third step in the founding process is to determine the representation rights. Representation rights can be issued, for example, to the company's CEO and chairman to represent and sign the company's documents digitally. There can be different kinds of representation rights for different occasions. Representation rights type can be, for example, "joint," which means that the individual can represent the company with other "joint" type company members. "Single" type of representation right could be issued, for example, to the CEO, which could single-handedly sign documents and contracts for the company.

These digital representation rights are assigned as verifiable credentials, as shown in Figure 12. Digital representation rights can be provided basically to any person as long as they have a DID. In this case, representation rights can be provided to chosen stakeholders based on their DIDs, which they gave as a part of the founding documents signing process. The company can issue verifiable representation right credentials to chosen representatives by using the company's own DID as an issuer, and the representatives own DID as an upcoming owner of the representation rights. When the representative has received the representation rights from the company, the verifiable credential needs to be accepted by countersigning and storing the presentation rights.

6.1.6 Shareholder authorization to debit equity

The minimum share capital to found an LLC in Finland is 2500 euros and this capital must be debited to the LLC's bank account before registering the company. (PRH 2018). The minimum share capital requirement is applicable for companies founded before the first of July 2019. Companies founded past this date are released from the minimum capital requirement and the following process steps. (PRH 2019b)

In the fourth step, the company's shareholders will authorize the company's FI to debit equity from their bank accounts, but the amount is not yet debited at this stage. Shareholders can review the equity debit details and then approve that the company's FI can debit equity from shareholders' accounts. This authorization request is sent to all shareholders by the FI.

This process is completed by using Open Banking APIs, and it is authorized by using DIDs and verifiable claims. It is extremely important to prove that the authorization was truly initiated by the shareholder since we are initiating bank payment from the shareholder to the company's bank account.

The financial institution which the LLC uses creates a PSD2 based authorization request based on the shareholders and their ownership structure. The authorization request includes all the necessary information which is needed to debit equity from the shareholder's bank account. This contains the DIDs of the company and shareholder, IBAN bank account numbers of both company and founder, debited amount, and authorization proof from the shareholder.

Shareholders fill the required information which results in the authorization proof. The authorization proof is signed with the shareholder's DID. Shareholder's FI can verify the DID and the identity of the shareholder if it is the same DID which the shareholder uses when using other FI's services. Signed authorization proof is sent back for storage to the FI which the company uses. The company's FI then mediates the authorization proof back to the shareholder's FI and request access tokens to the shareholder's account's payments API. Shareholder's FI verifies the received proof and its signatures by using the DID and fetching the public key from the DDO, which is written on the Hyperledger Indy, identity ledger. Again, the public key is used to verify the signature and to identify that the identity holder is the shareholder and the account owner. When the signature and identity is verified, the shareholder's bank can provide API access token generated with the specifications of the

authorization proof to the company's FI. An API access token can be used to get access to the payment's API of the shareholder's bank account to debit equity from the shareholder's bank account. This access token is stored by the company's FI for later use.

This process is repeated to other shareholders as well. The information is forwarded via Open banking APIs from all shareholders to FIs which they are using. During this stage, a similar authorization request is sent to the founder to pay the company registration fee to the registry official. This authorization request follows the same kind of procedure as described above.

6.1.7 Full KYC check

All involved participants can follow the company's founding process almost in real-time from the FI's service and see and verify the conducted signatures. The final KYC is conducted for stakeholders before completing the founding process.

The final KYC check is conducted manually by the KYC Brokering service before the company registration can be submitted. KYC Brokering service will revise and verify if any of the shareholders is PEP (Politically exposed person), that none of the stakeholders are in the sanction list, KRP/NBI asset freezing list and actual/ultimate beneficial ownership (UBO) of the company. KYC brokering service requires the full name of all stakeholders, date of birth, personal ID in case of Finnish ID is available, ownership amount, and position in the company.

After KYC brokering service has conducted the KYC process, a report will be created which points out success and failures for each point. All the points should success otherwise, the system will not allow the process to continue, and stakeholders who did not pass the KYC test should be changed or removed. When the KYC process is conducted successfully, the process can continue, and shareholders and board members are finalized.

6.1.8 Create a bank account and debit equity from shareholders

After the final KYC is successfully conducted the FI where the founder started the process will create a bank account for the newly founded company. The bank account is created

according to the internal processes of each financial institution. The company's FI can now debit equity on the shareholder's bank account since the FI already has authorization from the shareholders. This is done by using shareholder's FI's PSD2 payments APIs to request equity from the shareholder's bank account to the company's bank account. The equity payment request is processed and executed by the shareholder's FI, which transfers the funds to the company's bank account based on the ownership amount. The company's FI registers the payment when it has received the funds.

When the equity is debited from all shareholders, the company's FI will create proof that the equity is paid in full. This proof is stored with the founding documents and sent to the trade registry office to verify that the equity is fully paid, and the company can be registered by the registry office.

6.1.9 Verification and registration

The company can now create a new DID for itself, and now not only the stakeholders have a DID but the newly founded company as well. Before the final registration, the trade registry office needs to validate the submitted documents. This is done by using their internal process and by verifying all the DID documents by requesting public keys from the Indy ledger. This is done by using the stakeholders DIDs which were used in the registration process. The trade registry officials need to verify the signatures in the founding documents as described in Figure 17. The trade registry also needs to verify the proofs of equity payments as well as the registration payment by verifying the digital signatures of the proof.

When the trade registry official has conducted the verification process, the founding documents are stored by trade registry officials, and legal identifiers are created. The company can now use the founding documents as a verifiable claim for business purposes. The trade registry official also creates representation rights credentials for the proposed representatives which were nominated in the founding documents.

The trade registry officials share the trade registration information to tax administration, which registers the company according to their internal processes. Finally, the trade registry official informs other parties in the network that the founding process is successfully finished.

At this stage, the founder is notified on the web portal that the company is successfully founded and the company receives founding documents and legal identifiers as verifiable digital claims which are used for business purposes. The newly founded company’s DID is now written to the Indy ledger by the FI and the company is founded fully digitally.

7 INVESTMENT ANALYSIS SIMULATION

Investment analysis simulation is conducted to understand the profitability of Project Mercury for the case company. Risk and uncertainty are an intrinsic part of investments, and thus the Monte Carlo-based simulation approach is used to better include the uncertainty by including different scenarios.

In this chapter, the results of the investment analysis simulation are presented and discussed. The results of the simulation are shown in the summary statistics and visualized by using NPV, DPP and IRR distributions for the investment. This investment analysis is conducted from the point of view of a financial institution that was part of Project Mercury.

7.1 Net present value

Monte Carlo-simulation indicates that the average and median net present value for Project Mercury is positive. The average NPV is 601 000 euros, and the median NPV is 561 000 euros which can be seen from Table 13 below. However, the distribution of possible net present values are relatively wide as can be seen from Figure 18 below. The minimum NPV for the project is approximately –1 616 000 euros and the maximum NPV is approximately 3 205 000 euros. The standard deviation of 776 000 euros is relatively large. This indicates the riskiness of the project and also the uncertainty related to the estimated cash flows.

The simulation indicates that more than ¾ of all simulated NPV values are positive. The net present value distribution is not completely normally distributed since the skewness indicates a positive skew as the right tail is longer. Therefore, the median NPV is lower than the average NPV. A low kurtosis value of -0,2682 indicates that there are no extreme values in either tail, which can be also seen visually from Figure 18 below.

SUMMARY STATISTICS				
Number of iterations	10000		Minimum NPV	-1 615 961 €
Average NPV	601 114 €		Median NPV	560 979 €
Standard deviation	775 635 €		Maximum NPV	3 205 021 €
Skewness	0,2636		Percentage of negative NPVs	23,41 %
Kurtosis	-0,2643		Percentage of positive NPVs	76,59 %

Table 13. Summary statistics for the net present value

The net present value distribution in Figure 18 below presents visually the simulated net present values. The red bar indicates negative values, the grey bar indicates values that are close to zero (+/- 100 000e) and blue bar indicates positive net present values. Based on the simulated net present values the investment is profitable on average, but there is a large variation between different scenarios.

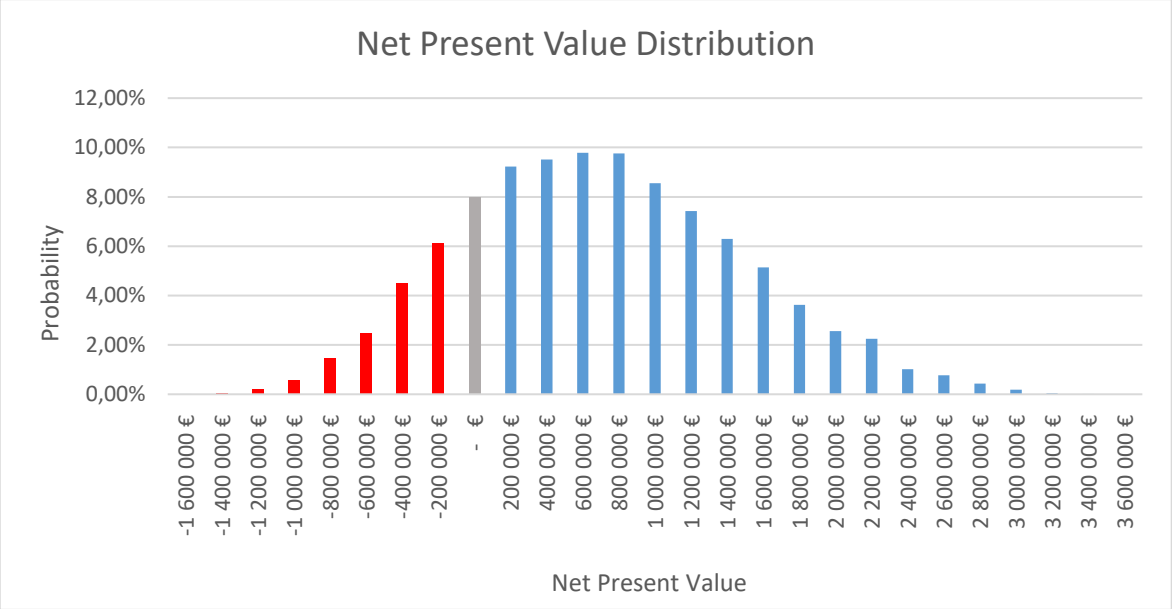

Figure 18. Net present value distribution

7.2 Internal rate of return

The internal rate of return simulation produces a relatively similar value distribution as was seen with the net present value distribution. The average and median internal rate of return for Project Mercury is positive. The average IRR is 3,68 % and the median IRR is 3,38 % which can be seen from Table 14 below. The distribution of the possible internal rate of return values is wide, as it was with the NPV values. The minimum IRR for the project is -9,86 % and the maximum IRR is approximately 24,90 %. Standard deviation gives a value of 4,71 %. The IRR simulation gives relatively similar results with the NPV simulation, which is due to the similarity with the two equations.

The simulation indicates again that more than ¾ of all simulated NPV values are positive. The net present value distribution is not completely normally distributed since the skewness indicates a positive skew as the right tail is longer. Therefore, the median IRR is lower than

the average IRR. A low kurtosis value of -0,0285 indicates that there are no extreme values of either tail, which can be also seen visually from Figure 19 below.

SUMMARY STATISTICS			
Number of iterations	10000	Minimum IRR	-9,86 %
Average IRR	3,68 %	Median IRR	3,38 %
Standard deviation	4,71 %	Maximum IRR	24,90 %
Skewness	0,3441	Percentage of negative IRRs	22,92 %
Kurtosis	0,0285	Percentage of positive IRRs	77,08 %

Table 14. Summary statistics for internal rate of return

The internal rate of return value distribution below in Figure 19 presents visually the simulated IRR values. Red bar indicates negative IRR values, the grey bar indicates values that are close to zero (+/- 0.5 %) and the blue bar indicates positive IRR values. Based on the simulated IRR values the investment is profitable on average, but there is a large variation between simulated values. On average the simulated IRR values are relatively low, which is partly due to the high discount rate used in the simulation.

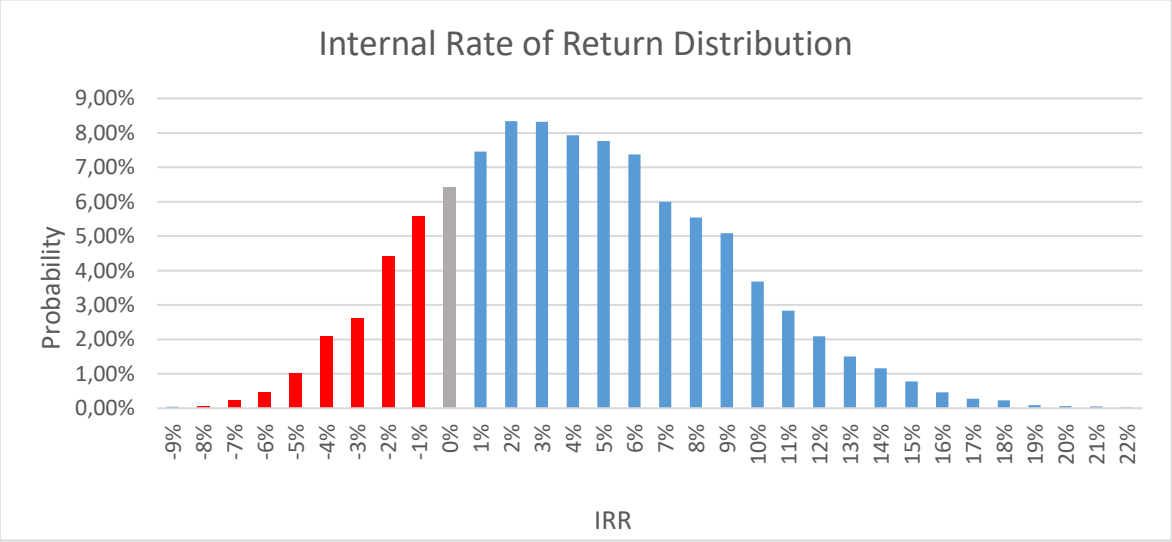

Figure 19. Internal rate of the return distribution

7.3 Discounted payback period

The average and median discounted payback period indicate approximately 12 years of discounted payback for the investment. The average DPP is approximately 12,8 years and the median DPP 12,1 years which can be seen from Table 15 below. These values can be

seen as relatively long payback periods since it is not taking into account the investments without a payback. If the discounted payback period was more than 25 years it is assumed that the investment will not payback itself. The distribution of possible discounted payback periods is very wide as can be seen from figure 20 below. The minimum DPP for the project is approximately 4,5 years and the maximum DPP period which is still considered as a payback is 25 years. The standard deviation is 4,45 years which indicates a lot of variation between the simulated values. The simulation indicates that more than ¾ of all simulated DPP will actually pay back the investment. The net present value distribution is not normally distributed since the skewness is high and indicates strong positive skewness. Kurtosis indicates that the distribution is not normally distributed and there are relatively high values in both tails of distributions.

SUMMARY STATISTICS				
Number of iterations	10000		Minimum DPP	4,37
Average DPP	12,81		Median DPP	12,06
Standard deviation	4,45		Maximum DPP	24,03
Skewness	0,6684		Percentage of DPPs over 25 years/No Payback	22,76 %
Kurtosis	-0,3408		Percentage of positive DPPs	77,24 %

Table 15. Summary statistics for the discounted payback period

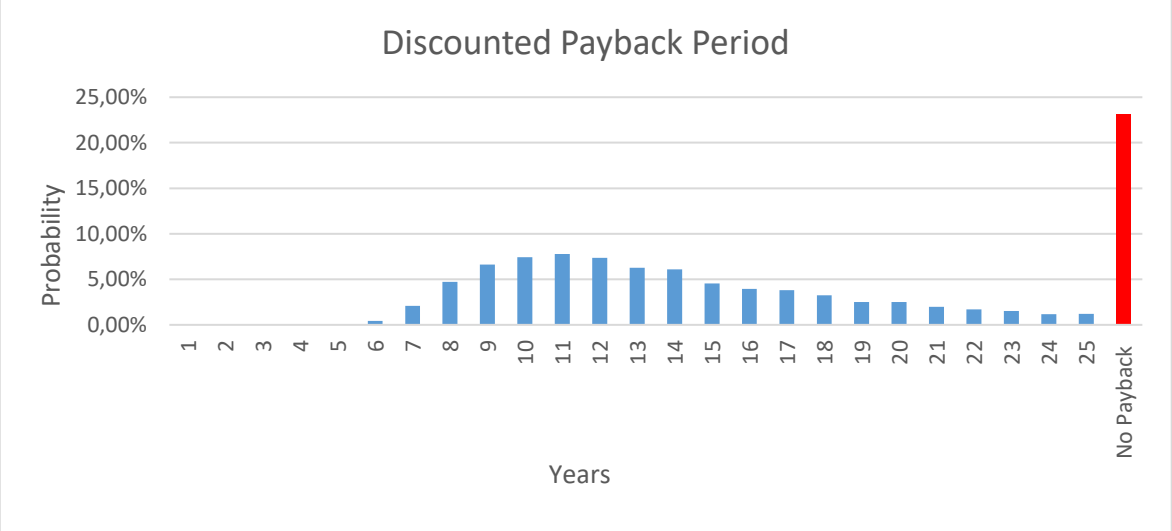

Figure 20. Discounted payback period distribution

7.4 Discussion and summary of results

NPV and IRR simulation indicated positive values approximately in ¾ of simulated values. The average NPV was 601 000 euros, but IRR values were relatively low, on average 3,68 %. The discounted payback period revealed that there is a high possibility that the payback period is relatively long, more than ten years. The average and median payback period indicated a payback time of more than 12 years without taking account investments without a payback.

The distributions also revealed that the possible NPV, IRR and DPP distributions for all the simulated values are relatively wide. This is due to the large variation between the minimum and maximum input-values, which affected the simulated values. This means that there is a lot of uncertainty related to future cash in and outflows. A high discount rate drastically lowered all simulated metrics, but it should be also kept in mind that Project Mercury holds a lot of risks.

The project is hedging the risk by sharing the investment into different stages, two proof of concepts (Project Mercury and Project Jupiter) and then piloting these projects before the possible commercial service. The feasibility of the project is assessed and evaluated after each stage to minimize the risks and invested capital. In addition to that, the Project Mercury shared the costs amongst each other which made the initial cost of the proof of concept relatively low.

Project Mercury was seen more as a research and development cost in the case company, and thus, no direct revenues were expected from the project. The future cash flows are challenging to estimate for Project Mercury since most of the revenues are indirect and would come from the increased number of new customers. Project Mercury is only a part of larger investments towards distributed ledger technologies in the case company. There are various proof of concepts within the same field that overlaps each other and makes it difficult to assign the costs and revenues for different projects. This signifies the need for the simulation-based approach because of the increased difficulty to assign cost and future revenues to Project Mercury. Due to the overlapping of different proof of concepts, project Jupiter is also included in this investment analysis simulation since they are closely linked together, and Project Mercury acted as a foundation for Project Jupiter.

7.5 Value propositions of Project Mercury

Based on the illustrative case study and investment analysis simulation the value proposition of project Mercury can be discussed. Project Mercury demonstrated how a limited liability company could be founded entirely digitally, based on distributed ledger technologies. During the Project Mercury, DLT-based digital document signing and processing were introduced, and a new kind of self-sovereign digital identity was created for all entities in the network. DLT technologies made it possible for founders to initiate and complete the company founding process from their end-device without any physical interaction or manual paperwork. This speeded up the founding process, made it more user-friendly and made it possible to remove all the manual paperwork associated with the founding process.

In the process of digitalizing the company's founding process, a self-sovereign digital identity was created for the newly established company. The SSI enables the company to be reliably identified and to share verified data related to it. The SSI also makes it easier to manage the company since the company can authorize its employees to represent the company digitally. For example; “various different accounts could be opened for the company, the company can be registered for VAT and Tax Administration prepayment register, the Patent and Registration Office can register the company, and the company can manage its shareholder register entirely digitally.” (Project Mercury 2018)

Currently, it is not possible to update the company information to authorities, financial institutions and to other stakeholders simultaneously and in real-time. However, with the use of distributed ledger technology, the authorities are part of the same business network, and the company information can be sent to all parties in the network, practically in real-time. The use of distributed ledger and SSI makes it possible to share reliable and verifiable information in real-time related to the LLC to every party in the network. This makes the information flow flawlessly between all parties and the company management process more efficient.

SSI enables globally accessible digital identity for limited companies that could be represented by employees with globally verifiable representation rights. The company itself could also found, for example, a new company in a highly transparent way. Project Mercury also concluded that while the PoC was developed in collaboration with Finnish companies,

the technological solution is not geographically limited since it is based on open-source distributed ledger technologies and thus the basic principles could be applied everywhere.

This new kind of founding process can be seen as more attractive for the company founder and stakeholders, which could give a competitive advantage for FIs that are offering this kind of service. This could increase the number of new customers, and with the use of cross-selling of other financial services, multiplier effects might be achieved. Therefore, the possible financial benefits in the form of cash inflows could come indirectly from the increased number of new customers, especially new business customers and synergies that are achieved by Project Mercury. KYC costs could be overall decreased on the network level since the company stakeholders need to be strongly identified only once by one of the financial institutions which are part of the business network. After the strong identification, the financial institution which accomplishes the KYC process can issue a verifiable claim to the company stakeholder, which could be used in all authentication procedures in all organizations which are part of the business network.

The value proposition of Project Mercury can be divided into two main categories. Firstly, it speeded and eased the founding process of a limited liability company and secondly, after the company was founded, it made the company management process more efficient. However, the broader impact could come from the future applications and opportunities that the digital identity for the company enables.

7.6 Future impact and applications of Project Mercury

Distributed ledger technology and SSI should be seen as a broader context, and the digital company founding process is only one of the numerous possible applications for SSI and DLT. By bringing together the two key innovations; decentralized transaction management, and decentralized identity data management, it is possible to digitalize contracts and signatures and by that way create new business models as was shown in Project Mercury.

The digital identity and verifiable claims could be extended beyond the founding process and in premise, could always be applied when verifiable proofs need to be presented. This could mean digitalizing all credentials from driving licenses, identification cards, passwords, usernames, powers of attorney to academic diplomas and so on. Anytime when a credential needs to be used it could be digitalized in the same way as was shown in Project Mercury.

The signing of founding documents is also only one example of a contract that could be digitalized and signed in a decentralized way. Again, there are numerous contracts that could be signed digitally by using the same principles applied in Project Mercury. Therefore, the implications of Project Mercury go way beyond the company's founding process. With this in mind, there are numerous different applications, and instead of thinking only one application this should be seen as a broader context; decentralized data ecosystem.

Therefore, the broader impact could probably come from future applications after the LLC is founded digitally and has a digital identity. Due to the digitalization of the company identity and its shareholder register, the company's shares could be digitalized and tokenized. This could enable a globally digitally verifiable and traceable ownership structure without the need for centralized parties.

Project Jupiter is a continuum from Project Mercury. The aim of Project Jupiter is to create a fully decentralized trade network for non-listed company shares. Project Mercury acted as a foundation for Project Jupiter, which could be built-on. Project Jupiter demonstrates how issuance and trading on non-listed company shares can be fully digitalized. Digital identity with digitally verifiable and traceable ownership structure enables the trading of unlisted company shares in the Corda-network. Project Jupiter demonstrates three core functionalities of the network: Founding share issuance, founding round, and trading of shares.

This network enables companies, shareholders, and investors to trade and manage non-listed company shares. Project Jupiter includes private and public entities, creating a market-driven, legally compliant network of services. This creates a market opportunity for both primary and secondary services related to non-listed shares. As a second proof of concept, this also strengthens the feasibility of the Corda and Indy-based digital company network.

Currently, the shares of unlisted companies are illiquid, and this kind of service could increase the liquidity of unlisted shares, thus introducing a new asset class to asset management services. This could be a significant disruption in corporate equity finance. The value of this market is enormous in the Finnish scale. The estimated value of unquoted shares held by Finnish households is 61 billion euros, and enterprises and non-profits are estimated to own approximately shares worth of 130 billion euros. Together accounting almost 200 billion worth of value which can be seen from Table 16 below. (Project Jupiter 2019)

Value of unlisted shares	Entity
61 Billion Euros	Finnish households
130 Billion Euros	Enterprises and nonprofits
348 Million Euros	Investments into Finnish startups and early-stage growth companies

Table 16. The value of unlisted shared held by different entities in Finland

The buying and selling of unlisted shares are manual activity and there are only a couple of secondary marketplaces for unlisted shares which only account for a fraction of the total amount of unlisted shares. As a result, this asset class lacks liquidity which affects the value of unlisted shares. For highly illiquid assets, the value is lower since the security cannot be easily traded into cash by using its fair market value. Therefore, increased liquidity often increases the value of an asset. This is known as the liquidity premium phenomenon. The liquidity premium is high for most of the unlisted shares thus decreasing the market value of the shares. Due to the increased liquidity, financing for unlisted companies becomes easier and the shares could be used as a collateral asset.

Project Jupiter offers a new opportunity to develop and maintain the primary and secondary marketplace for non-listed shares for service providers. A better understanding of the value of unlisted shares and up to date information related to the ownership structure of unlisted companies makes it possible to form a better picture of both shareholders as well as the company's wealth. This means that FIs that are part of the network could offer better wealth management and advisory services for clients with unlisted shares and even new products for investors which would prefer to invest in them.

Public authorities benefit from Project Jupiter as well since they get higher quality and up-to-date information related to the ownership structure of companies and to conducted trades. Markets become more transparent, and real-time information enables real-time taxation and register updates. According to Project Jupiter this "can be seen as a good example of public-private co-operation where administrative burden can be reduced".

8 CONCLUSION AND DISCUSSION

In this chapter, the conclusion of the thesis is discussed, and the research questions that were presented in the introduction chapter are answered. Critique and limitations of this thesis are outlined and at the end of this chapter, possible future research objectives are presented.

8.1 Conclusion

This illustrative case study studied on how distributed ledger technology could be used as a catalyst for digitalizing the founding process of a limited liability company. The current process of founding an LLC is very manual and time consuming for the company stakeholders and involved entities. The purpose of the Project Mercury was to explore how the founding process could be digitalized and improved for all involved entities by using distributed ledger technologies. Distributed ledger technologies are a relatively new phenomenon and according to the literature review Project Mercury was the first time when the digital company founding process was demonstrated with DLT. This emphasizes the novelty of the Project Mercury and so the apparent research gap which this thesis is endeavoring to fill by answering the research questions presented in the introduction chapter:

Question 1: *How the founding process of a limited liability company can be digitalized with the use of DLTs?*

DLT technologies made it possible for founders to initiate and complete the company founding process from their end-device by using a web service without any physical interaction or manual paperwork. The founding process of a limited liability company can be digitalized by digitalizing contracts and signatures which are used in the founding process. Essentially, the founding document and its signing process need to be digitalized. Contracts can be digitalized by using DLT as a decentralized transaction management ledger and signatures by using a scalable identity ledger for digital signatures. Self-sovereign identity with new kinds of decentralized identifiers (DIDs) can be used for identity purposes and digital signatures. Distributed ledger technology enabled the authorities to be part of the company founding process and company information can be shared with all parties in the network, practically in real-time. The use of distributed ledger and SSI makes it possible to

share reliable and verifiable information in real-time related to the LLC to every party in the network. This makes the information flow flawlessly between all parties and the company founding process more efficient.

1.1 Which are the main DLT-ledgers used in Project Mercury, and what are these ledgers used for?

Project Mercury used Corda as a distributed ledger for recording, managing, and automating legal agreements between business partners and, thus, it acted as a backbone of the network between different entities. Corda is inspired by blockchain technology but it neither has any built-in cryptocurrency and nor does it use or store data in blocks. Corda uses partial visibility, which means that the transactions happen point-to-point which underlines the issues related to scalability, privacy, and governance that hinders the adoption of blockchain technology. Corda is not a public system and it uses “notary services” to provide transaction ordering and timestamping services. Notary services ensure that no double-spending of transactions is happening and notaries are expected to be run by multiple mutually distrusting parties.

Hyperledger Indy is used as a distributed ledger for managing self-sovereign digital identities for all entities in the network. Self-sovereign identity is an identity that is controlled by the user. Hyperledger Indy is an identity network that is used for DIDs and verifiable claims. The self-sovereign identity uses verifiable claims to proof aspects related to the identity owner. This could be for example qualification, driving license, government ID, or university degree. DIDs are identifiers used in SSI and are under the control of the identity owner. DIDs are used for secure interaction with the identity holder. Hyperledger Indy with the use of DIDs can also be used for decentralized digital document signing. Indy network is used for identity purposes only, all other information related to sharing and agreement handling is conducted by using the Corda network. Two different ledgers were used since the requirements for identity, and the managing of agreements are very different.

1.2 How can a self-sovereign identity be created for a limited liability company?

In the process of digitalizing the company's founding process, a self-sovereign digital identity was created for the newly established company. The SSI enables the company to be reliably identified and to share verified data related to it. The SSI also makes it easier to manage the company since the company can authorize its employees to represent the company digitally.

Self-sovereign identity can be created for the company in the same way as it is created for other identity holders. First, a trusted party, FI in this scenario issues a verifiable claim for the company which the company can use to prove its identity. Financial institutions can issue this claim to the company since the company data and company stakeholders are strongly identified by the FI and information broker during the founding process of a company. The company can use this issued claim to present itself since the verifiers already have an existing trust relationship with the issuer of the identity.

Question 2: *What is the estimated profitability of Project Mercury for the case company?*

Investment analysis simulation was conducted for the case company which was a Project Mercury participant from the financial industry. Project Mercury is not expected to generate direct revenues, but the revenues are estimated to occur indirectly from the increased amount of both business and private customers due to the improved digital company founding and management processes. Cost savings are expected to occur, from more efficient processes, especially from the KYC processes, since company stakeholders are only needed to be identified once in the business network.

The major sources of costs are expected to occur first from the proof of concept, then from the pilot and finally from the fully working service. These investments are made in stages and the feasibility to continue is evaluated after each stage. When the production-ready service is operating there are estimated to occur operating costs increasing 3 % per annum. The exact triangular input-value distributions used in the simulation can be found in Tables 9 and 10.

Monte Carlo-based investment analysis simulation revealed that approximately 75 % of the simulated NPV and IRR values are positive. The average NPV for the investment is

approximately 600 000 euros and median approximately 560 000 euros. The average internal rate of return for the investment is 3,68 percent and the median value is 3,38 percent. However, there is a wide deviation between the simulated results; the maximum simulated NPV gave a result of 3 200 000 euros and the minimum – 1 600 000 euros.

The minimum IRR is -9,86 % and the maximum is 24,9 %, which indicates that it is difficult to predict the profitability of this investment. In the extreme scenarios, the difference can be immense, however, the probability for extreme results is very low. In addition, a closer examination revealed that the average discounted payback period for the investment is 12,8 years and median 12 years. NPV, IRR and DPP distributions with the summary statistics can be found from chapter six.

In light of these results could be argued that the IRR for the investment is relatively low and the discounted payback period relatively long. Also, when taking into account the high risk and high variation between different simulated values the project holds a high risk, but relatively low return.

However, there are various variables that affect the results. The investment analysis was conducted in accordance with the precautionary principle, which in practice means that the risks were outlined while the opportunities were carefully included by using a high discount rate. The high discount rate decreased the values of future cash flows, especially so since for the first three years there were no cash flows expected, only expenses. This should be taken into account when interpreting results.

Question 3: *What are the implications of Project Mercury for different stakeholders?*

Company stakeholders: For company stakeholders, the DLT-technologies made it possible to initiate and complete the company founding process from their end-device without any physical interaction or manual paperwork. This speeded up the founding process, made it more user-friendly and made it possible to remove all the manual paperwork associated with the founding process. The SSI enables the company to be reliably identified in various contexts and to share verified data related to it. The SSI also makes it easier to manage the company since the company can authorize its employees to represent the company digitally. SSI enables globally accessible digital identity for limited companies that could be

represented by employees with globally verifiable representation rights. The company itself could also found, for example, a new company in a highly transparent way.

Authorities: Currently, it is not possible to update company information to both authorities, financial institutions or other stakeholders simultaneously and in real-time. However, with the use of distributed ledger technology, the authorities are part of the same process, and company information can be sent to all parties in the network, practically in real-time. The use of distributed ledger and SSI makes it possible to share reliable and verifiable information in real-time related to the LLC to every party in the network. This makes the information flow flawlessly between all parties and the company management process more efficient.

Financial institutions: This new kind of founding process can be seen as more attractive for the company founder and stakeholders, which could give a competitive advantage for financial institutions that are offering this kind of digital service. Digital service could increase the number of new customers, and with the use of cross-selling of other financial services, multiplier effects might be achieved. Therefore, the possible financial benefit in the form of cash inflows could come indirectly from the increased number of new customers, especially new business customers. KYC costs could be overall decreased on the network level since the company stakeholders need to be strongly identified only once by one of the financial institutions which are part of the business network. After the strong identification, the financial institution which accomplishes the KYC process can issue a verifiable claim to the company stakeholder, which could be used in all authentication procedures in all organizations which are part of the business network.

3.1 What are the future implications and opportunities of Project Mercury?

Distributed ledger technology and SSI should be seen as a broader context, and the digital company founding process is only one of the numerous possible applications for SSI and DLT. By bringing together the two key innovations, decentralized transaction management, and decentralized identity data management, it is possible to digitalize contracts and signatures and in that way create new business models as was shown in Project Mercury.

The digital identity and verifiable claims could be extended beyond the founding process and in premise, could always be applied when verifiable proofs need to be presented. This

could mean digitalizing all credentials from driving licenses, identification cards, passwords, usernames, powers of attorney to academic diplomas and so on. Anytime when a credential needs to be used it could be digitalized in the same way as was shown in Project Mercury.

The signing of founding documents is also only one example of a digital contract which could be digitalized and signed in a decentralized way. Again, there are numerous contracts that could be signed digitally by using the same principles applied by Project Mercury. Therefore, the implications of Project Mercury go way beyond the company's founding process.

Therefore, the broader impact could probably come from future applications after the LLC is founded digitally and has a digital identity. Due to the digitalization of the company identity and its shareholder register, the company’s shares could be digitalized and tokenized. This could enable a globally digitally verifiable and traceable ownership structure without the need of centralized parties.

Project Jupiter is a continuum from the Project Mercury. The aim of the Project Jupiter is to create a fully decentralized trade network for non-listed company shares. Project Mercury acted as a foundation for Project Jupiter, which could be built-on. Project Jupiter demonstrates how issuance and trading on non-listed company shares can be fully digitalized. Digital identity with digitally verifiable and traceable ownership structure enables the trading of unlisted company shares in the Corda-network. Project Jupiter demonstrates three core functionalities of the network: Founding share issuance, founding round, and trading of shares.

Currently, the shares of unlisted companies are illiquid, and this kind of service could increase the liquidity of unlisted shares which, could be a significant disruption in corporate equity finance. The estimated value of unquoted shares held by Finnish entities is almost 200 billion. DLT-based network and service could increase the liquidity and thus the value of these shares.

8.2 Critique and Limitations

As this research is based on the proof of concept and the technology is still in a relatively nascent stage there are various elements that can change in the future. Currently, there are

no working decentralized identity networks in existence, which could support millions of users. This means that the technological solutions used in Project Mercury could change when this technology matures. Neither there are de facto solutions to store the cryptographic keys related to the signing of transactions which can hinder especially the adoption of self-sovereign identity. If the identity holder is not managing the private keys associated with the identity, it is not a truly self-sovereign identity. In addition, if the keys are lost the identity is lost with the keys. There are various different key recovery solutions proposed, but it is out of the scope of this research.

One important question is to ponder whether the founding process of an LLC could be digitalized without the use of DLT. It is very likely that the founding process can be digitalized without DLT based technologies, however, the key advantage of DLT-based solutions is that there is no central authority that tracks the records, and thus there is no "single point of failure" as it is in traditional databases. This results in a reliable source of data that is robust to system failures and that cannot easily be tampered. DLT allows parties to maintain shared, synchronized and accurate records without having to trust each other fully since the data is not controlled by a single entity. Therefore, DLT enables data and assets to move between different parties flawlessly and eliminates the process of reconciliation and duplication of data. (Brown 2016)

The investment analysis simulation holds various limitations. The input-values for the Monte Carlo simulation were challenging to estimate since the Project Mercury was in a proof of concept stage. Future cash flows associated with the Project Mercury are mostly estimated to come from indirect cash flows and projects which are built on top of Project Mercury. The Project Mercury itself is not expected to bring direct revenues which made estimating the profitability of Project Mercury more challenging. Also, the costs associated with Project Mercury are challenging to estimate since there are various projects which overlap each other and make the allocation of costs very challenging. There is a lot of uncertainty related to the estimated input-values for the Project Mercury which can be seen from the NPV, IRR and DPP distributions. At this stage, it is very challenging to estimate the profitability of Project Mercury and the final profitability of the investment can radically change compared to the estimated values.

8.3 Further research objectives

The contingent research object which arises from this thesis is the future implications of Project Jupiter, the continuum of the Project Mercury. One research objective would be to study on a deeper level on how the decentralized trade network for non-listed company shares can be carried out and what are the broader implications on different stakeholders. In addition, one interesting research subject would be to study the effects of liquidity premium on unlisted shares in Finland since Project Jupiter could increase the liquidity of these shares.

The simulation-based investment analysis presented in this thesis could be conducted again in the near future to achieve more accurate results. The input values used in this thesis incorporate a lot of uncertainty, since the Project was in a proof-of-concept stage. When there is more certainty related to the input-values and understating what input values to include, the simulation could be run again.

The research subjects, self-sovereign identity and DLT are relatively new concepts and thus offer plenty of new research objectives. SSI gives users the control to manage their own data, however, at the same time, it leaves the user to be responsible for their own security. Therefore, different SSI key recovery schemes could be studied and compared since it is an essential part to make SSI fully functioning, especially so if public blockchains are used.

DLT could be also studied in the context of back-office processes. One interesting research objective would be to study if DLT could be applied in the back-office processes in financial institutions. DLT could be used to tokenize the units of mutual funds. Also, the whole subscription and redemption process of mutual funds could be contemplated, if the process could be made more straightforward and remove third parties from the process. The ideal situation would be to remove the back-office as a whole if asset managers could make the subscriptions and redemptions directly to fund management. In theory, this with the tokenization of funds could make the subscription and redemption process to work in real-time and cut a significant amount of costs.

REFERENCES

Abraham, A. Theurman, K. Kirchengast, E. 2018. Qualified eID Derivation into a Distributed Ledger Based IdM System. Conference paper. 17th IEEE International Conference on Trust, Security, and Privacy in Computing and Communications

Allen, C. 2016. The Path to Self-Sovereign Identity. [online document]. [Accessed 1 June 2019]. Available at http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Allen, C. Brock, A. Buterin, V. Callas, J. Dorje, D. Lundkvist, C. Kravchenko, P. Nelson, J. Reed, D. Sabadello, M. Slepak, G. Thorp, N. Wood, H. 2015. Decentralized public key infrastructure. *A White Paper from Rebooting the Web of Trust.* [online document]. [Accessed 1 June 2019]. Available at https://danubetech.com/download/dpki.pdf

Andrianto, Y. Diputra, Y. 2018. The effect of cryptocurrency on investment portfolio effectiveness. *Journal of Finance and Accounting,* 229 – 237

Androulaki, E. Karame, G. Roeschlin, M. Scherer, T. Capkun, S. 2013 Evaluating user privacy in Bitcoin. *Business and information systems engineering,* Volume 59, Issue 3, 183- 187

Baur, D. Hong, K. Lee, A. 2018 Bitcoin: Medium of exchange or speculative assets? *Journal of International Financial Markets, Institutions & Money,* Vol 54, 177.

Beerens, M. 2018. Could blockchain be a bigger disrupter than the internet [online document]. [Accessed 1 June 2019]. Available at https://www.investors.com/etfs-and-funds/etfs/blockchain-technology-bigger-internet/

Belin, O. 2019. The difference between blockchain and distributed ledger technology [online document]. [Accessed 1 May 2019] Available at: https://tradeix.com/distributed-ledger-technology/

Bencic, F. Skocir, P. Zarko, I 2019. DL - Tags: DLT and Smart Tags for decentralized, privacy-preserving and verifiable supply chain management. *IEEE Access 05 April 2019,* 1 – 1

Bent, F. 2006. Five Misunderstandings About Case-Study Research. *Qualitative Inquiry*, vol. 12, no. 2. pp. 219-245

Bloomberg 2019. German Government Bonds 10Yr Dbr. GDBR10:IND [online document]. [Accessed 11 Oktober 2019]. Available at https://www.bloomberg.com/quote/GDBR10:IND

Bollen, R. 2013. The legal status of online currencies: Are Bitcoins the future? *Journal of Banking and Finance Law and Practise.* [online document]. [Accessed 1 June 2019]. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2285247

Brauneis, A. Mestel, R. 2018. Cryptocurrency-portfolios in a mean-variance-framework. *Finance Research Letters.* 1-5.

Briére, M. Oosterlinck, K. Szafarz, A. 2015. Virtual currency, tangible return: Portfolio diversification with Bitcoin. *Journal of Asset Management*, Vol 16 (6), 1-14

Brown, R. 2016. On Distributed Databases and Distributed Ledgers. Thoughts on the future of finance. [online document]. [Accessed 1 June 2019]. Available at https://gendal.me/page/2/

Brown, R. 2018. The Corda platform: an introduction. [online document]. [Accessed 1 June 2019]. Available at https://www.corda.net/content/corda-platform-whitepaper.pdf

Brown. R, Carlyle, J. Grigg, I. Hearn, M. 2016. Corda: an introduction. [online document]. [Accessed 28 August 2019]. Available at https://www.researchgate.net/publication/308636477_Corda_An_Introduction/link/57e994ed08aed0a291304412/download

Buterin, V. 2013. A Next-Generation Smart Contract and Decentralized Application Platform. [online document]. [Accessed 1 June 2019]. Available at https://github.com/ethereum/wiki/wiki/White-Paper

Buterin, V. 2017a. Introduction to Cryptoeconomics. [online document]. [Accessed 1 June 2019]. Available at https://vitalik.ca/files/intro_cryptoeconomics.pdf

Buterin, V. 2017b. Sharding – FAQ. Scalability trilemma. [online document]. [Accessed 1 June 2019]. Available at https://github.com/ethereum/wiki/wiki/Sharding-FAQ

Cali, U. Cakir, O. 2019. Energy policy instruments for distributed ledger technology empowered peer-to-peer local energy markets. *IEEE access*, Vol.7, pp 82888-82900

Cameron, K. 2005. The Laws of Identity. [online document]. [Accessed 1 August 2019]. Available at https://msdn.microsoft.com/en-us/library/ms996456.aspx

Chauhan, A. Malvuya, O. Verma, M. Mor, T. 2018. Blockchain and scalability. *IEEE International conference on software quality, reliability and security companion.*

Cheah, E-T. Fry, J. 2015. Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. *Economics Letters*, 32-35.

Chodhury, A. Shankar, R. Tiwari, M. 2005. Consensus-based intelligent group decision-making model for the selection of advanced technology. *Decision support systems* Vol.42(3) pp.1776-1799

Coelho, P. Zuquete, A. Gomes, H. 2018. Federation of Attribute Providers for User Self-Sovereign Identity. *Journal of information systems engineering and management,* 2, 6.

Coinmarketcap. 2019. Top 100 Cryptocurrencies by Market Capitalization. [online document]. [Accessed 1 August 2019]. Available at https://coinmarketcap.com/

Conradt, L. Roper, T. 2005. Consensus decision making in animals. *Trends in Ecology and Evolution.* Vol.20(8), pp.449-456

Corda. 2019a. Corda homepage. [online document]. [Accessed 1 August 2019]. Available at https://www.corda.net/

Cronin, A. 2015. Individual and group personalities characterize consensus decision-making in an ant. *Ethodology.* Vol.121(7) pp.703-713

Cronin, A. Stumpe, M. 2014. Ants work harder during consensus decision-making in small groups. *Journal of the Royal Society, Interface*. Vol.11(98) pp.20140641

Damodaran, A. 2014. Session1:Introduction to valuation. [online document]. [Accessed 25 October 2019]. Available at https://www.youtube.com/watch?v=znmQ7oMiQrM

Damodaran, A. 2019. Weighted average cost of capital by industry sector. [online document]. [Accessed 3 August 2019]. Available at http://people.stern.nyu.edu/adamodar/New_Home_Page/datacurrent.html#discrate

Daoyuan, S. 2010. The application of Monte Carlo computer simulation in investment risk analysis. *IEEE Conference publication.*

Der, U. Jähnichen, S. Sürmeli. J. 2017. Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution. [online document]. [Accessed 1 August 2019]. Available at https://arxiv.org/abs/1712.01767

Devlin, F. Guinan, P. 2017. Blockchain: revolution, regulation, and the way forward. *The RMA Journal.* Vol. 100(1). 48 – 51

Dewey, J. Emerson, M. 2017. Beyond Bitcoin: How distributed ledger technology has evolved to overcome impediments under the uniform commercial code, *Uniform Commercial Code Law Journal,* Vol 47(2), 105

Dougherty, C. 2008. MD5 vulnerable to collision attacks. Carnegie Mellon University. [online document]. [Accessed 1 August 2019] Available: https://www.kb.cert.org/vuls/id/836068/

Dunphy, P. Petitcolas, F. 2018. A First Look at Identity Management Schemes on the Blockchain. *IEEE Security and Privacy.* Vol16(4), 20-29

Dwyer, G. 2015. The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability,* Vol 17, 81-91

Dyer, J. Ioannou, C. Morrell, L. Croft, D. Couzin, I. Waters, D. Krause, J. 2008. Consensus decision making in human crowds. *Animal Behaviour*. Vol 75(2), 461-470

Dyhrberg, A. 2016. Bitcoin, gold, and the dollar – A Garch volatility analysis. *Finance Research Letters*, Vol 16, 85-92.

Ehrsam, F. 2017. Scaling Ethereum to billions of users [online document]. [Accessed 1 August 2019]. Available at https://medium.com/@FEhrsam/scaling-ethereum-to-billions-of-users-f37d9f487db1

Ellis, S. Juels, A. Nazarov, S. 2017. ChainLink. A decentralized oracle network. [online document]. [Accessed 1 August 2019]. Available at https://link.smartcontract.com/whitepaper

Eriksson, P. Kovalainen, A. 2008. "Qualitative Methods in Business Research". 2 edition. Sage Publications Ltd. London: Sage.

Eskola, J. Suoranta, J. 2000. Johdatus laadulliseen tutkimukseen. Tampere. Vastapaino.

Etherscan. 2019. Block #0. [online document]. [Accessed 2 July 2019]. Available at https://etherscan.io/block/0

Fearon, J. (1999) What is identity (as we now use the word)? *Department of political science. Standford University.* [online document]. [Accessed 2 July 2019]. Available at: https://web.stanford.edu/group/fearon-research/cgi-bin/wordpress/wp-content/uploads/2013/10/What-is-Identity-as-we-now-use-the-word-.pdf

Federal Trade Commission 2019. Affected by the Equifax breach? File a claim now. [online document]. [Accessed 7 June 2019]. Available at https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement

Ferdous, Md-S. Chowdhury, F. Alassafi, M – O. 2019. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access 2019, Vol.7, pp.1033059 - 103079

Ferraro, P. King, C. Shorten, R. 2018. Distributed ledger technology for smart cities, the sharing economy, and social compliance. *IEEE Access*, Vol. 6, 62728 – 62746

Finanssialan Keskusliitto 2013. Tupas identification service identification principles. Version 2.0c [online document]. [Accessed 7 June 2019]. Available at https://www.finanssiala.fi/maksujenvalitys/dokumentit/TUPAS_identification_principles_v20c.pdf

Fischer, I. (1907) The rate of interest. Its nature, determination and relation to economic phenomena. The Mac Millan company. New York.

Fisher, C. 2010. Researching and Writing a Dissertation: An Essential Guide for Business Students. Pearson Education Limited. Edinburgh Gate, Harlow.

Gartner. 2018. 5 Trends emerge in the Gartner hype cycle for emerging technologies, 2018. [online document]. [Accessed 2 July 2019]. Available at https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

Gaspars-Wieloch, H. 2017. Project Net present value estimation under uncertainty. *Central European journal of operations research.* Vol. 27. Issue 1. Pp. 179-197.

Gerring, J. What is a case study and what is it good for? *The American Political Science Review* Vol. 98, No. 2 pp. 341-354

Google Scholar. 2019. Web search engine [online document]. Available at https://scholar.google.com/

Google Trends. 2019. Search Term: Blockchain [online document]. [Accessed 1 July 2019]. Available at https://trends.google.fi/trends/explore?date=all&q=blockchain

Grigalucas, T. Chang, Y. Luo, Meifeng. 2002. Containerport investment appraisal and risk analysis: Ilustrative case study. Vol.1782(1) pp.64-72.

Gruner, A. Muhle, A. Gayvoronskaya, T. Meinel, C. 2018. A Quantifiable Trust Model for Blockchain-based Identity Management. *IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics. Conference publication.*

Guo, L. Wang, Y. 2018. Cryptocurrency: A new investment opportunity? *The Journal of Alternative Investments.* pp.16-36.

Guodong, C. 2013. Based on monte carlo simulation investment portfolio VaR risk analysis. *Journal of convergence information technology*. Vol.8(9), 1071

Haddoudi, S. Ech-Cherif, E. Dafir, M. 2019. Analysis of identity management systems using blockchain technology. *Conference* paper. International Conference on Advanced Communication Technologies and Networking (CommNet)

Harju, N. 2017. CGI. Lohkoketjujen anatomia – osa 8: Erilaisuus on rikkaus. [online document]. [Accessed 1 May 2019]. Available at https://www.cgi.fi/fi/blogi/lohkoketjujen-anatomia-osa-8-erilaisuus-on-rikkaus.

Hayes, R. Kyer, B. Weber, E. 2015. The case study cookbook. [online document]. [Accessed 1 May 2019]. Available at https://web.wpi.edu/Pubs/E-project/Available/E-project-121615-164731/unrestricted/USPTO_CookbookFinal.pdf

Hearn, M. 2016. Corda: a distributed ledger. Version 0.5 [online document]. [Accessed 1 May 2019]. Available at https://www.corda.net/content/corda-technical-whitepaper.pdf

Hileman, Dr. Rauchs, M. 2017. Global blockchain benchmarking study. [online document]. [Accessed 1 May 2019]. Available at https://cdn.crowdfundinsider.com/wp-content/uploads/2017/09/2017-Global-Blockchain-Benchmarking-Study_Hileman.pdf

Hirsjärvi, S. Hurme, H. 2001. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki. Helsinki University Press.

Hoffman, F. Wurster, S. Eyal, R. Bohmecke-Schwafert, M. 2017. The immutability concept of blockchains and benefits of early standardization. *IEEE Conference Publications*

Hotti, T. 2017. The age of decentralization in the world of silos. OP Financial Group. [online document]. [Accessed 1 May 2019]. Available at https://www.vtt.fi/sites/BOND/SiteCollectionDocuments/The%20Age%20of%20Decentralization%20in%20the%20World%20of%20Silos%20Timo%20Hotti.pdf?fbclid=IwAR02qvkpZ3Xeg02m02WWeXRGiXmUW6GO9zfPXhP116QFbXE6ygogykHZC9o

Hu, J. 2019. Learn blockchain's top 25 hacks in history. Hackernoon. [online document]. [Accessed 2 July 2019]. Available at https://hackernoon.com/tech-explained-top-24-blockchain-hacks-in-history-first-half-40c390dc4a96

Hyperledger 2019a. About Hyperledger. [online document]. [Accessed 2 July 2019]. Available at https://www.hyperledger.org/about

Hyperledger 2019b. Hyperledger. [online document]. [Accessed 2 July 2019]. Available at: https://www.hyperledger.org/

Hyperledger 2019c. Hyperledger Indy. [online document]. [Accessed 2 July 2019]. Available at https://www.hyperledger.org/projects/hyperledger-indy

Hyperledger 2019d. Hyperledger Indy Github. [online document]. [Accessed 2 July 2019]. Available at https://github.com/hyperledger/indy-node/blob/master/README.md

Hyperledger 2019e. Hyperledger projects. [online document]. [Accessed 2 July 2019]. Available at https://www.hyperledger.org/projects

Hyperledger 2019f. Plenum Byzantine fault-tolerant protocol. [online document]. [Accessed 2 July 2019]. Available at https://github.com/hyperledger/indy-plenum/wiki

Hyperledger Indy 2019. Hyperledger Indy Wiki. [online document]. [Accessed 8 December 2019] Available at https://wiki.hyperledger.org/display/indy/Hyperledger+Indy

Idfy 2019. Idfy Identification principles. Finnish Trust Network (FTN) [online document]. [Accessed 8 December 2019]. Available at https://www.idfy.io/company/finnish-trust-network/

Ikäheimo, S. Laitinen, E. Laitinen, T. Puttonen, V. 2011. Laskentatoimi ja rahoitus. Vaasan Yritysinformaatio Oy. Vaasa.

Jeffries, A. 2018. Blockchain is meaningless. *Report*. [online document]. [Accessed 2 July 2019]. Available at https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning

Klimos, P. 2018. The distributed ledger technology: a potential revamp for financial markets? *Capital Markets Law Journal.* Vol 13(2), pp 194-222

Kotz, S. Van Dorp, J. 2004. Beyond Beta: Other continuous families of distributions with bounded support and applications. World Scientific Publishing Co, Singapore.

KPMG. 2018. Blockchain could create new opportunities for verified identity solutions. *International Financial Law Review.*

Kuo, T-T. Kim, H-E. Ohno-Machado, L. 2017. Blochain distributed ledger technologies for biomedical and health care applications, *Journal of the American Medical Informatics Association,* Vol24(6), 1211-1220

Lake, P. Crowther, P. 2013. Concise Guide to Databases: A Practical Introduction. Springer.

Lee, H. Teichroeb, J. 2016. Partially shared consensus decision making and distributed leadership in vervet monkeys: older females lead the group to forage. *American Journal of Physical Anthropology.* Vol.161(4), pp.580-590

Liu, B. Yu X. Chen, S. Xu, X. Zhu, L. 2017. Blockchain based data integrity service framework for IoT data, *IEEE International Conference on Web Services*, 469

LUT Finna. 2019. Databases. [online document]. [Accessed 2 July 2019]. Available at https://wilma.finna.fi/lut/Browse/Database

Manning, M. Sutton, M. Zhu, J. 2016. Distributed ledger technology: in securities clearing and settlement: some issues. *JASSA*, Issue 3, 30-36.

McCrank, J. Finkle, J. 2018 Equifax breach could be most costly in corporate history. Reuters. [online document]. [Accessed 23 August 2019]. Available at https://www.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUSKCN1GE257

Metropolis, N. Stanislaw, U. 1949. The Monte Carlo Method. *Journal of the American Statistical Association*. Vol. 44, No.247. pp. 335–341.

Microsoft Azure 2017. Federated Identity pattern. [online document]. [Accessed 23 August 2019]. Available at https://docs.microsoft.com/en-us/azure/architecture/patterns/federated-identity

Mills, A. J. Durepos, G. Wiebe, E. 2010. Encyclopedia of Case Study Research, Volumes I and II. Thousand Oaks, CA: Sage

Mills, D. Wang, K. Malone, B. Ravi, A. Marquardt, J. Chen, C. Badev, A. Brezinski, T. Fahy, L, Liao, K. Kargenian, V. Ellithorpe, M. Ng, W. Baird, M. 2016. Distributed ledger technology in payments, clearing and settlement. *Finance and economics discussion series 12/2016,* Vol.2016(095)

Mohanty, D. (2019) R3 Corda for architects and developers. With case studies in finance, insurance, healthcare, travel, telecom, and agriculture. Apress. India.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system [online document]. [Accessed 23 August 2019]. Available at https://bitcoin.org/bitcoin.pdf

Nordseth, G. 2009. Solution profile – significant identity services. *European federated validation service study* [online document]. [Accessed 23 August 2019]. Available at http://ec.europa.eu/idabc/servlets/Doc43ad.pdf?id=32174

Parra Moyano, J. Ross, O. 2017. KYC Optimization using distributed ledger technology. *Business and information systems engineering*, Vol.59(6), 411-423

Piekkari, R. Welch, C. Paavilainen, E. 2009. The case study as disciplinary convention: Evidence from international business journals. *Organizational Research Methods*, 12(3): 567–589.

Platon, V. Contantinescu, A. 2014. Monte Carlo method in risk analysis for investment projects. *Procedia Economics and Finance*. Vol.15, pp.393-400

PRH 2019a. Changes – limited liability companies. [online document]. [Accessed 5 September 2019]. Available at https://www.prh.fi/en/kaupparekisteri/muutokset_rekisteritietoihin/limitedcompanyamendments.html

PRH 2018. Choose the type of your business. . [online document]. [Accessed 23 September 2019]. Available at https://www.prh.fi/en/kaupparekisteri/yrityksen_perustaminen/forms_of_business.html

PRH 2019b. Osakeyhtiö, asunto-osakeyhtiö ja keskinäinen kiinteistöosakeyhtiö: Vaatimus osakepääomasta poistuu 1.7.2019. [online document]. [Accessed 8 December 2019]. Available at https://www.prh.fi/fi/kaupparekisteri/osakeyhtio/osakeyhtion_asunto-osakeyhtion_ja_keskinaisen_kiinteistoosakeyhtion_osakepaaomavaatimus_poistuu_1.7.2019.html

Project Jupiter. 2019. Jupiter Slush pitch deck. Internal material. Not publicly available.

Project Mercury. 2018. Project Mercury internal workshop material. Not publicly available.

Prybila, C. Schulte, S. Hochreiner, C. Weber, I. 2017. Runtime verification for business processes utilizing the Bitcoin blockchain. *Future Generation Computer Systems.*

Pyöriä. P. 2018. Samlink Finnish Trust Network OIDC security key and data exchange process between brokers and identity providers. Samlink Oy. V. 0.8 [online document]. [Accessed 8 December 2019]. Available at https://www.samlink.fi/wp-content/uploads/2019/02/Avaintenhallinta.pdf

Qin, R. Yuan, Y. Wang, F. 2018. Research on the selection strategies of blockchain mining pools. *IEEE Transations and computional social systems.* Vol 5(3), 748-757

R3 (2019a) About. Website. [online document]. [Accessed 5 May 2019]. Available at: https://www.r3.com/about/

R3 (2019b) History. Website. [online document]. [Accessed 5 May 2019]. Available at: https://www.r3.com/about/

Reed, D. 2017. ONC DC Blockchain code-a-thon office hours by Souvrin. [online document]. [Accessed 23 August 2019]. Available at https://www.youtube.com/watch?v=1rXRCseYgYY

Reed, D. 2018. The story of open SSI standards – Drummond Reed/Evernym. SSIMeetup.org. [online document]. [Accessed 30 August 2019]. Available at https://www.youtube.com/watch?v=RllH91rcFdE&t=656s

Reed, D. Law, J. Hardman, D. 2017. The technical foundations of Sovrin. *A white paper from the Sovrin Foundation*. 4-25

Reed, D. Sporny, M. Longley, D. Allen, C. Grant, R. Sabadello, M. 2019. Decentralized identifiers (DIDs) v0.13. Final community group report 13 August 2019. [online document]. [Accessed 23 August 2019]. Available at https://w3c-ccg.github.io/did-spec/

Remer, D. Nieto, A. 1995. A compendium and comparison of 25 project evaluation techniques. Part 1: Net present value and rate of return methods. *International Journal of Production economics.* Vol. 42 Issue 1. Pp.79-96

Reza, S. Nguyen, T. Aijun, A. 2018. A new approach to client onboarding using self-sovereign identity and distributed ledger. *Conference Publications.*

Ridder, H-G. 2017. The theory contribution of case study research designs. Business research. Springer.

Sekiguchi, K. Chiba, M. Kashima, M. 2018. The securities settlement system and distributed ledger technology. *IDEAS working paper series from RePEc*

Sermpinis, T. Sermpinis, C. 2018. Traceability decentralization in Supply chain management using blockchain technologies. [online document]. [Accessed 23 August 2019]. Available at https://arxiv.org/ftp/arxiv/papers/1810/1810.09203.pdf

Sharma, T. 2018. How is blockchain verifiable by public and yet anonymous. [online document]. [Accessed 23 August 2019]. Available at https://www.blockchain-council.org/blockchain/how-is-blockchain-verifiable-by-public-and-yet-anonymous/

Siano, P. De Marco, G. Rolan, A. Loia, V. 2019. A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets. *IEEE Systems Journal*, 19 March 2019, pp. 1-13

Simon, M. 2011. Assumptions, Limitations and delimitations. *Dissertation and scholarly research: Recipes for success (2011 Ed.).*

Soltani, R. Trang Nquyen, U. An, A. 2018. A new approach to client onboarding using self-sovereign identity and distributed ledger. *IEEE Conference publications.*

Sovrin 2019. Stewards. [online document]. [Accessed 23 August 2019]. Available at https://sovrin.org/stewards/

Sovrin. 2018. Sovrin™: A protocol and token for self-sovereign identity and decentralized trust. *A White Paper from the Sovrin Foundation*. 4 – 42

Stokkink, Q. Pouwelse, J. 2018. Deployment of a blockchain-based self-sovereign identity. *IEEE Conference publications.*

Sultan, K. Ruhi, U. Lakhani, R. 2018. Conceptualizing blockchains: Characteristics and applications. *11th IADIS international conference information systems.*

Sumpter, D. Krause, J. James, R. Couzin, I. Ward, A. 2008. Consensus decision making by fish. *Current biology*. Vol.18(22),pp.1773-1777

Swan, M. 2015. Blockchain: Blueprint for a new economy. First Edition. O'Reilly Media.

Szabo, N. 1997. The idea of smart contracts. [online document]. [Accessed 1 July 2019]. Available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

Takemiya, M. Vanieiev, B. 2018. Sora Identity: secure, digital identity on the blockchain. *Conference paper.* Computer Software and Applications Conference (COMPSAC).

Taylor, R. Thomas-Gregory, A. 2015. Case study research. *Nursing standard. Royal college of nursing (Great Britain) Vol.29 (41), 36-40*

The U.S. Government Accountability Office. 1990. Case study evaluations. [online document]. [Accessed 23 August 2019]. Available at https://www.gao.gov/special.pubs/10_1_9.pdf

TrafiCom 2019. Electronic identification. [online document]. [Accessed 8 December 2019]. Available at https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/electronic-identification

Tziralis, G. Kirytopoulos, K. Rentizelas, A. Tatsiopoulos, I. 2009. Holistic investment assessment:optimization, risk appraisal and decision making. Managerial and decision economics. Vol.30(6) pp.393-403

UK Government. 2016. Distributed ledger technology: beyond block chain. [online document] [Accessed 1 July 2019] Available at

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Uwe, A. Özgur, Y. 2015. Economic risk analysis of decentralized renewable energy infrastructures – A Monte Carlo Simulation approach. *Renewable Energy*, Vol.77, pp.227-23

Voshmgir, S. 2017. Disrupting the governance with blockchains and smart contracts. *Strategic Change* Vol.26(5), 499-509

W3C 2019. Decentralized Identifiers (DIDs) v0.10. Data model and Syntaxes for Decentralized Identifiers (DIDs). *W3C Community Group Final Report* [online document] [Accessed 1 July 2019] Available at https://w3c-ccg.github.io/did-spec/

Webster, J. Watson, R. 2002. Analyzing the past to prepare for the future: Writing A Literature Review. *MIS Quarterly*. Vol26(2), 13–23.

Wei, J. Jian, Z. Jianglan, L. 2011. Mining investment risk analysis based on monte carlo simulation. *Fifth international conference on management of e-commerce and e-government.*

Wei, J. Jian, Z. Jianglan, L. 2011. Mining investment risk analysis based on Monte Carlo simulation. IEEE Conference Publications.

Windley, P. 2017. Hyperledger welcomes project Indy. [online document] [Accessed 1 July 2019] Available at https://www.hyperledger.org/blog/2017/05/02/hyperledger-welcomes-project-indy

Windley, P. 2019. Decentralized identifiers. Phil Windley's technometria. . [online document]. [Accessed 23 August 2019]. Available at http://www.windley.com/archives/2019/02/decentralized_identifiers.shtml

Yin, R. 2013. Case Study Research: Design and Methods *(5th ed.). Thousand Oaks, CA: SAGE Publications.* ISBN 978-1-4833-2224-7.

Zhou, T. Li, X. Zhao, H. 2019. EverSSDI: blockchain-based framework for verification, authorization and recovery of self-sovereign identity using smart contracts. *International Journal of Computer Applications in Technology.* Vol.61(3)), pp.281-295

APPENDIXES

Appendix 1.

Read me and run the simulation

Master Thesis

Author:	Mikko Mäenpää
Title:	Digitalizing the founding process of a limited liability company by using distributed ledger technologies: A case study of the Project Mercury and its profitability analysis
Faculty:	School of Business and Management
Master's Program:	Strategic Finance and Business Analytics
Year:	2019
Master's Thesis:	128 Pages, 20 Figures, 16 Tables, 6 Equations, 4 Appendixes
Supervisors:	Mariia Kozlova, Pekka Kaipio, Timo Hotti
Examiners:	Mikael Collan, Mariia Kozlova
Keywords:	Distributed Ledger Technology, Self-Sovereign Digital Identity, Blockchain, Digitalization, Corda, Hyperledger Indy, Decentralized Identifier (DID), Sovrin, Investment Analysis, Monte Carlo-simulation

This Microsoft Excel-spreadsheet is conducted as a part of the master thesis process and its main objective is to be used as a tool to calculate the profitability of Project Mercury and Project Jupiter. The profitability of these projects is estimated by utilizing a Monte Carlo-based investment analysis simulation. The results of the simulations are interpreted using summary statistics and visualized by the net present value (NPV), internal rate of return (IRR), and discounted payback period (DPP) distributions. Input-values for the simulation are gathered by interviewing the Project Mercury participants with semi-structured interviews.

Input-values for the simulation can be found from the "INPUT VALUES"-sheet.
Discounted cashflows with recorded NPV, IRR and DPP values can be found from the "INVESTMENT ANALYSIS SIMULATION"-sheet
Results of the simulation interpreted with summary statistics tables and visualized with NPV, IRR and DPP distributions can be found from the "SUMMARY STAT. AND VISUALIZATION"-sheet.

Please note that the simulation can take a few minutes, depending on the computer's processing power and the amount of RAM-memory. Only one simulation should be run at a time. 10 000 simulations are used as a basis in this model

To run the particular simulation, please push but the button below:

NPV Simulation | IRR Simulation | DPP Simulation

Appendix 2.

Input-values for the simulation 1/4

PROJECT MERCURY (INPUT VALUES 1/4)

REVENUE PROJECT **MERCURY**

Indirect Revenues From New LLC Customers			
Minimum	100 000,00 €	**Result**	Random number
Most Likely	150 000,00 €	**220 549,17 €**	*0,4422*
Maximum	500 000,00 €		

Cost Savings From More Efficient Processes			
Minimum	30 000,00 €	**Result**	Random number
Most Likely	45 000,00 €	**125 161,94 €**	*0,9510*
Maximum	150 000,00 €		

INVESTMENT COST **MERCURY**

Proof of Concept			
Minimum	-50 000,00 €	**Result**	Random number
Most Likely	-60 000,00 €	**- 79 404,31 €**	*0,7879*
Maximum	-100 000,00 €		

Pilot			
Minimum 2x Poc	- 100 000 €	**Result**	Random number
Most Likely 3x Poc	- 180 000 €	**- 169 724,34 €**	*0,1519*
Maximum 5x Poc	- 500 000 €		

Commercial Service			
Minimum 7x Poc	- 350 000 €	**Result**	Random number
Most Likely 10 x Poc	- 600 000 €	**- 833 519,81 €**	*0,5708*
Maximum 15x Poc	- 1 500 000 €		

OPERATIONAL COSTS **MERCURY**

Operational Cost			
Minimum 20% Investment Cost	- 120 000,00 €	**Result**	Random number
Most Likely 25% Investment Cost	- 150 000,00 €	**- 131 802,07 €**	*0,0774*
Maximum 30% Investment Cost	- 180 000,00 €		

Input-values for the simulation 2/4

PROJECT JUPITER (INPUT VALUS 2/4)

REVENUE PROJECT **JUPITER**

Tokenization of Unlisted Shares			
Minimum	200 000,00 €	**Result**	Random number
Most Likely	300 000,00 €	**319 653,85 €**	*0,4579*
Maximum	500 000,00 €		

INVESTMENT COST **JUPITER**

Proof of Concept			
Minimum	-50 000,00 €	**Result**	Random number
Most Likely	-60 000,00 €	**- 69 255,62 €**	*0,5274*
Maximum	-100 000,00 €		

Pilot			
Minimum 2x Poc	- 100 000 €	**Result**	Random number
Most Likely 3x Poc	- 180 000 €	**- 279 575,88 €**	*0,6204*
Maximum 5x Poc	- 500 000 €		

Commercial Service			
Minimum 7x Poc	- 350 000 €	**Result**	Random number
Most Likely 10 x Poc	- 600 000 €	**- 972 753,33 €**	*0,7314*
Maximum 15x Poc	- 1 500 000 €		

OPERATIONAL COSTS **JUPITER**

Operational Cost			
Minimum 20% Investment Cost	- 120 000,00 €	**Result**	Random number
Most Likely 25% Investment Cost	- 150 000,00 €	**- 138 207,92 €**	*0,1842*
Maximum 30% Investment Cost	- 180 000,00 €		

Input-values for the simulation 3/4 and 4/4

DISCOUNT RATE (INPUT VALUES 3/4)

The real discount rate utilized in the analysis	15 %
Nominal discount rate	17 %
Inflation	1,5 %
Risk-free rate	-0,5 %
Total risk premium for the investment (a + b)	17,5 %
(a) The weighted average cost of capital	4,5 %
(b) Project risk premium	13,0 %

SIMULATION ITERATIONS (INPUT VALUES 4/4)

Iterations	10000

Appendix 3.

Discounted cash flows (1/2)

Year	0	1	2	3	4	5	6	7	8	9	10
COSTS											
INVESTMENT COST MERCURY											
PoC	- 57 649 €										
Pilot		- 309 217 €									
Commercial Service			- 1 063 092 €								
Total Investment Cost Mercury	- 57 649 €	- 309 217 €	- 1 063 092 €								
INVESTMENT COST JUPITER											
PoC	- 89 338 €										
Pilot		- 153 821 €									
Commercial Service			- 409 119 €								
Total Investment Cost Jupiter	- 89 338 €	- 153 821 €	- 409 119 €	- €	- €	- €	- €	- €	- €	- €	- €
OPERATIONAL COST MERCURY											
Operational Cost Mercury (3% increase per year)				- 152 347 €	- 156 917 €	- 161 625 €	- 166 473 €	- 171 467 €	- 176 612 €	- 181 910 €	- 187 367 €
OPERATIONAL COST JUPITER											
Operational Cost Jupiter (3% Increase per year)				- 161 154 €	- 165 988 €	- 170 968 €	- 176 097 €	- 181 380 €	- 186 821 €	- 192 426 €	- 198 199 €
TOTAL COSTS	- 146 987 €	- 463 038 €	- 1 472 211 €	- 313 500 €	- 322 905 €	- 332 593 €	- 342 570 €	- 352 847 €	- 363 433 €	- 374 336 €	- 385 566 €
REVENUES											
PROJECT MERCURY											
Indirect Revenues From New LLC Customers (5% increase per year)				165 807 €	174 097 €	182 802 €	191 942 €	201 540 €	211 617 €	222 197 €	233 307 €
Cost Savings from More Efficient Processes				77 679 €	77 679 €	77 679 €	77 679 €	77 679 €	77 679 €	77 679 €	77 679 €
PROJECTJUPITER											
Tokenization of Unlisted Shares (5% increase per year)				272 979 €	286 628 €	300 959 €	316 007 €	331 807 €	348 398 €	365 818 €	384 109 €
TOTAL REVENUES				516 465 €	538 404 €	561 440 €	585 628 €	611 026 €	637 693 €	665 694 €	695 095 €
Net Cash Flows	- 146 987 €	- 463 038 €	- 1 472 211 €	202 964 €	215 498 €	228 848 €	243 058 €	258 178 €	274 260 €	291 358 €	309 529 €
Discounted Cash Flows	- 146 987 €	- 401 696 €	- 1 107 976 €	132 513 €	122 058 €	112 447 €	103 607 €	95 473 €	87 984 €	81 086 €	74 731 €
Cumulated Discounted Cash Flows	- 146 987 €	- 548 682 €	- 1 656 659 €	- 1 524 145 €	- 1 402 088 €	- 1 289 641 €	- 1 186 033 €	- 1 090 560 €	- 1 002 576 €	- 921 490 €	- 846 758 €
Fraction Row	-	-	-	-	-	-	-	-	-	-	-
Net Present Value	- 227 404,53 €										
Internal Rate of Return	-2 %										
Discounted Payback Period	No Payback										

Discounted cash flows (2/2)

11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €
- 192 988 €	- 198 778 €	- 204 741 €	- 210 883 €	- 217 210 €	- 223 726 €	- 230 438 €	- 237 351 €	- 244 472 €	- 251 806 €	- 259 360 €	- 267 141 €	- 275 155 €	- 283 410 €	- 291 912 €
- 204 145 €	- 210 269 €	- 216 577 €	- 223 075 €	- 229 767 €	- 236 660 €	- 243 760 €	- 251 072 €	- 258 604 €	- 266 363 €	- 274 354 €	- 282 584 €	- 291 062 €	- 299 793 €	- 308 787 €
- 397 133 €	**- 409 047 €**	**- 421 318 €**	**- 433 958 €**	**- 446 977 €**	**- 460 386 €**	**- 474 198 €**	**- 488 423 €**	**- 503 076 €**	**- 518 168 €**	**- 533 713 €**	**- 549 725 €**	**- 566 217 €**	**- 583 203 €**	**- 600 699 €**
244 973 €	257 221 €	270 082 €	283 586 €	297 766 €	312 654 €	328 287 €	344 701 €	361 936 €	380 033 €	399 035 €	418 986 €	439 936 €	461 932 €	485 029 €
77 679 €	77 679 €	77 679 €	77 679 €	77 679 €	77 679 €	77 679 €	77 679 €	77 679 €	77 679 €	77 679 €	77 679 €	77 679 €	77 679 €	77 679 €
403 314 €	423 480 €	444 654 €	466 886 €	490 231 €	514 742 €	540 479 €	567 503 €	595 879 €	625 672 €	656 956 €	689 804 €	724 294 €	760 509 €	798 534 €
725 965 €	758 380 €	792 415 €	828 152 €	865 675 €	905 075 €	946 445 €	989 883 €	1 035 493 €	1 083 384 €	1 133 669 €	1 186 469 €	1 241 908 €	1 300 120 €	1 361 242 €
328 832 €	349 333 €	371 096 €	394 194 €	418 699 €	444 689 €	472 247 €	501 460 €	532 417 €	565 216 €	599 956 €	636 744 €	675 692 €	716 917 €	760 543 €
68 874 €	63 475 €	58 496 €	53 905 €	49 671 €	45 766 €	42 163 €	38 840 €	35 775 €	32 947 €	30 339 €	27 934 €	25 715 €	23 670 €	21 784 €
- 777 884 €	- 714 409 €	- 655 913 €	- 602 008 €	- 552 337 €	- 506 571 €	- 464 408 €	- 425 568 €	- 389 793 €	- 356 846 €	- 326 507 €	- 298 573 €	- 272 858 €	- 249 188 €	- 227 405 €
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Appendix 4.

NPV Simulation Excel VBA Macro

```
Sub NPV_SIMULATION()


' NPV simulation
    ' Selecting the correct input-values sheet in the Excel-file.
    Sheets("INPUT_VALUES").Activate
    ' Selecting the cell which specifies the number of simulations
    Iterations = Cells(22, 23)
    ' Changing the active sheet to investment analysis sheet in which the simulation is conducted.
    Sheets("INVESTMENT_ANALYSIS_SIMULATION").Activate
    ' Selecting the range where the NPV-values are stored (10 000 cells).
    ActiveSheet.Range("A47:A10046").Select
    ' Clearing the selected range.
    Selection.ClearContents
    ' Selecting the cell that shows the NPV-value.
    ActiveSheet.Range("B42").Select
    ' Copying the selected NPV-value.
    Selection.Copy
    ' For loop is conducted to copy, paste and store the NPV-values
    For X = 1 To Iterations
    ' Selecting the cell in which NPV-value is stored
    Cells(X + 46, 1).Select
    ' NPV-values is pasted and stored
    Selection.PasteSpecial Paste:=xlValues
    'Repeating the step above until the condition is fulfilled
    Next X
    ' Clearing the clipboard
    Application.CutCopyMode = False
    ' Message box
    MsgBox ("NPV Simulation successfully completed with " & Iterations & " simulations. Results can be
found from the summary statistics spreadsheet.")


End Sub
```

IRR Simulation Excel VBA Macro

```
Sub IRR_SIMULATION()

' IRR simulation
    ' Selecting the correct input-values sheet in the Excel-file.
    Sheets("INPUT_VALUES").Activate
    ' Selecting the cell which specifies the number of simulations
    Iterations = Cells(22, 23)
    ' Changing the active sheet to investment analysis sheet in which the simulation is conducted.
    Sheets("INVESTMENT_ANALYSIS_SIMULATION").Activate
    ' Selecting the range where the IRR-values are stored (10 000 cells).
    ActiveSheet.Range("C47:C10046").Select
    ' Clearing the selected range.
    Selection.ClearContents
    ' Selecting the cell that shows the IRR-value.
    ActiveSheet.Range("B43").Select
    ' Copying the selected IRR-value.
    Selection.Copy
    ' For loop is conducted to copy, paste and store the IRR-values
    For X = 1 To Iterations
    ' Selecting the cell in which IRR-value is stored
    Cells(X + 46, 3).Select
    ' IRR-values is pasted and stored
    Selection.PasteSpecial Paste:=xlValues
    'Repeating the step above until the condition is fulfilled
    Next X
    ' Clearing the clipboard
    Application.CutCopyMode = False
    ' Message box
    MsgBox ("IRR Simulation successfully completed with " & Iterations & " simulations. Results can be
found from the summary statistics spreadsheet.")

End Sub
```

DPP Simulation Excel VBA Macro

```
Sub DPP_SIMULATION()


' DPP simulation
    ' Selecting the correct input-values sheet in the Excel-file.
    Sheets("INPUT_VALUES").Activate
    ' Selecting the cell which specifies the number of simulations
    Iterations = Cells(22, 23)
    ' Changing the active sheet to investment analysis sheet in which the simulation is conducted.
    Sheets("INVESTMENT_ANALYSIS_SIMULATION").Activate
    ' Selecting the range where the DPP-values are stored (10 000 cells).
    ActiveSheet.Range("E47:E10046").Select
    ' Clearing the selected range.
    Selection.ClearContents
    ' Selecting the cell that shows the DPP-value.
    ActiveSheet.Range("B44").Select
    ' Copying the selected DPP-value.
    Selection.Copy
    ' For loop is conducted to copy, paste and store the DPP-values
    For X = 1 To Iterations
    ' Selecting the cell in which DPP-value is stored
    Cells(X + 46, 5).Select
    ' DPP-values is pasted and stored
    Selection.PasteSpecial Paste:=xlValues
    'Repeating the step above until the condition is fulfilled
    Next X
    ' Clearing the clipboard
    Application.CutCopyMode = False
    ' Message box
    MsgBox ("DPP Simulation successfully completed with " & Iterations & " simulations. Results can be
found from the summary statistics spreadsheet.")


End Sub
```