An exploration and characterisation of public blockchain generations

the introduction of a characterisation framework highlighting the essential design considerations to select a public permissionless blockchain technology for blockchain use cases

van der Pasch, M.M.A.

Award date:
2018

Rabobank

An exploration and characterisation of public blockchain generations

The introduction of a characterisation framework highlighting the essential design considerations to select a public permissionless blockchain technology for blockchain use cases

Name: M.M.A. (Mark) van der Pasch *Student Number: 0944065*

MSc Innovation Sciences, *Department of Industrial Engineering & Innovation Sciences*

Publishing date: *July 1st, 2018*

1st supervisor: *prof. dr. B.M. Sadowski (Department of Industrial Engineering & Innovation Sciences)*

2nd supervisor: *prof. dr. G.M. Duysters (Department of Management, Tilburg University)*

3th supervisor: *prof. dr. Z.O. Nomaler (Department of Industrial Engineering & Innovation Sciences)*

TU/e Technische Universiteit Eindhoven University of Technology
Where innovation starts

An exploration and characterisation of public blockchain generations

The introduction of a characterisation framework highlighting the essential design considerations to select a public permissionless blockchain technology for blockchain use cases

Keywords: Blockchain, Exploration, Characterisation, Use cases, Framework, Bitcoin, Ethereum, Cardano, Blockchain Generations, Distributed Ledger Technology (DLT)

In partial fulfilment of the requirements for the degree of:

MSc Innovation Sciences

Department of Industrial Engineering & Innovation Sciences (IE&IS)

Eindhoven University of Technology

Date of Submission: July 1st, 2018

Author: M.M.A. (Mark) van der Pasch

Student number: 0944065

First supervisor: prof. dr. B.M. Sadowski (Department of Industrial Engineering & Innovation Sciences)

Second supervisor: prof. dr. G.M. Duysters (Department of Management, Tilburg University)

Third supervisor: prof. dr. Z.O. Nomaler (Department of Industrial Engineering & Innovation Sciences)

Company: Rabobank

Company coach: D.S. Baars, MSc

TU/e Technische Universiteit Eindhoven University of Technology

Where innovation starts

Rabobank

Disclaimer

The copyright of the master thesis lies with the author. The author is responsible for its contents. Additionally, this master thesis does not represent the public opinion of the Rabobank Group or any of the other involved companies nor their employees.

Management summary

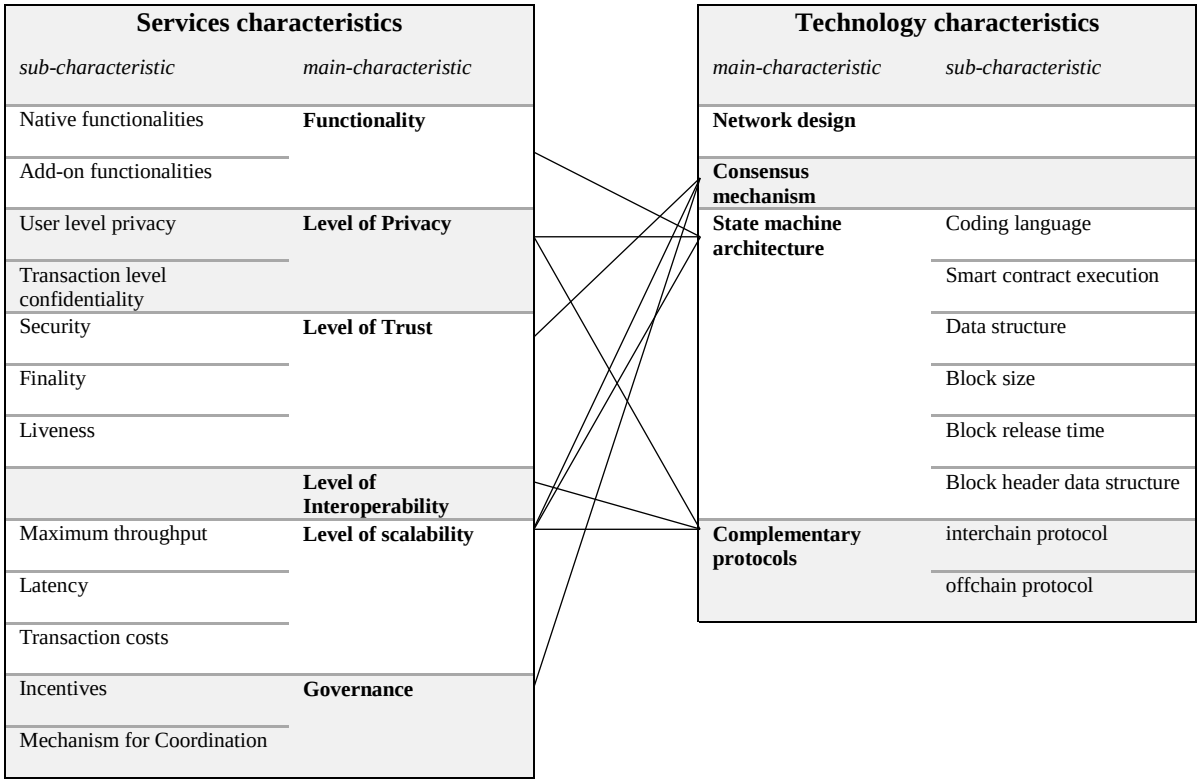
Blockchain technology and in broader terms distributed ledger technology, is a digital platform top trend in the Gartner hype cycle of 2017. Technology platforms, like Bitcoin and Ethereum, have much news attention; however, the underlying technology blockchain is still in infancy. According to Tapscott & Tapscott (2017), the technology behind blockchain technology is pulling the world in a new era of openness, decentralization and global (economic) inclusion. Due to the high potential of the technology, many enterprises are looking how to deal with this new technology. A person or group with the pseudonym Satoshi Nakamoto wrote a paper that conceptualizes the first generation blockchain application called Bitcoin. Nakamoto (2008) introduced "A purely peer-to-peer version of electronic cash that allows on-line payments to be sent directly from one party to another without going through a financial institution" (Nakamoto, 2008, p. 1). Back then in 2008, the full potential of blockchain was still unclear, however currently blockchain technology appears to become the foundation technology that leads to a fundamental change from trusting humans to trusting machines, and from centralized to decentralized control (Aste, Tasca , & Matteo, 2017). Towards the end of 2013, Vitalik Buterin who was a young programmer and Bitcoin enthusiast, started working on a project to expand the features of Bitcoin. He mentioned that multiple projects, such as Bitcoin, Namecoin, Peercoin and Mastercoin were limited in features and were mainly focused on fulfilling one particular feature. His vision was to build a universal blockchain solution, enabling multiple features on a single blockchain platform. Therefore, Ethereum is considered as a second-generation blockchain platform enabling multiple features.

Since there is much overlap and discussion about how to qualify the different type of blockchain technologies, this research builds on three type definitions for blockchain technologies:

- *Public permissionless*: everybody is allowed to access and participate in the blockchain, and everyone is allowed to participate in the consensus mechanism. Examples of this type are Bitcoin and Ethereum.
- *Public permissioned*: everybody is allowed to access and participate in the blockchain, however participation in the consensus mechanism is restricted. An example is Ripple.
- *Private permissioned:* The network is only accessable for a authorized group of users, and participation to the consensus mechanism is also restricted. Examples of this type are Hyperledger Fabric and Quorum.

This research focusses on public permissionless blockchains. In order to truly grasp the benefit and understand blockchain technology, this research introduces a characterisation framework based on Saviotti & Metcalfe (1984) ideology describing a technology as a set of service and technology characteristics that are interlinked by a pattern of mapping. A multiple case study describing Bitcoin, Ethereum and Cardano is used to draft this framework. Cardano claims to become a generation three-blockchain platform. The framework can be used to qualify the innovation output of public permissionless blockchain technologies. Table 0.1 provides an overview of the framework without a specific case filled in.

Table 0.1 A characterisation framework for public permissionless blockchains



The case study conducted for this research provided an overview of the current technical challenges of public permissionless blockchain technologies. Summarizing, the technical challenges of public blockchain technologies are related to the following service characteristics.

- *Level of Privacy:* The level of privacy is a challenge for public permissionless blockchain technologies. User accounts on public permissionless blockchains are pseudonymous and the transactions are open and accessible. However, several protocols are currently introduced to improve the level of transaction confidentiality, i.e. zkSNARKs.
- *Level of Trust:* Although the level of trust is considered high for Bitcoin and Ethereum, both protocols do not enable absolute finality, which is required for some use cases. This challenge relates to the current Proof of Work consensus mechanism implementation. The proposed Proof of Stake implementation of Ethereum will potentially solve this challenge.
- *Level of Interoperability:* Currently, the three studied blockchain technologies do not enable native mechanism to interconnect heterogeneous blockchains. Currently the proposed solutions are mostly complementary protocols such as side-chains that enable a connection between two blockchain platforms.
- *Level of Scalability:* One of the most debated issues is scalability. Public blockchains currently have low throughput and high cost per confirmed transactions. This is the trade-off for decentralized computations. Currently, several technology solutions are proposed that potentially increase the level of scalability of Ethereum, i.e. Sharding, Casper, Plasma.
- *Governance:* Governance can be distinguished in off-chain and on-chain governance. Currently, much of the governance occurs off-chain by a selected group of participants. A truly democratic system would be in place where each stakeholder has equal voting rights. Such a system is very complex and brings multiple challenges. A solution opposed for on-chain delegated voting is the liquid democracy model however, this solutions seems far from integration. Another challenge for blockchain use cases is that the price of the system cannot be predicted due to cryptocurrency price fluctuations.

Besides qualifying the current state and challenges of public permissionless blockchain technologies, the framework can be used as a guideline to define the technology design considerations for a blockchain use case. It should be noted that the framework only applies to the design choices regarding the selection of a technology.

Above insights are used in order to answer the main research question addressed in this paper. The main research question addressed by this research is '*How to qualify public permissionless blockchain technologies and why are these not wide-scale adopted for business use cases?'*

Blockchain technology is currently in a hype; however, production ready public permissionless blockchain use cases are scarce. Several reasons for this are identified. Firstly, current public permissionless blockchain technologies have many technical challenges and these challenges are mentioned in chapter 5.4. Currently, the open source communities are putting much effort in solving the technological challenges and therefore this research strongly recommends companies to follow the developments regarding public permissionless blockchains closely in order to not miss the boat. Secondly, public permissionless blockchain technologies have a high level of trust, are decentralized and are secure; this has trade-offs for scalability. Therefore, the technology solution design of blockchain use cases should be as minimalistic and efficient as possible. Thirdly, the technology behind blockchain is only a small part of a blockchain use case. Many other decisions required for a business use case introduce many other (non-technical) challenges, such as legal in relation to the general data protection regulation (GDPR), compliance and off-chain governance. Questions like 'who is responsible?' and regarding the price volatility of cryptocurrency often occur and have to be solved. Fourthly, blockchain technology enables new forms of collaboration between people and businesses and this sometimes feels scary, this implies that new business models have to be explored that enable new types of collaborations. Besides the challenges, public permissionless blockchains create many opportunities regarding new or more efficient business models. It should be noted that corporates are currently investigating many public permissioned blockchains and corresponding use cases. During the research, Rabobank went live with the we.trade platform, which is a private permissioned blockchain platform based on Hyperledger Fabric. Both public permissioned and private permissioned blockchain types are out of scope of this research.

References

Aste, T., Tasca , P., & Matteo, T. D. (2017). The Foreseeable Impacton Society and Industry. *IEEE Computer Society*, 18-28.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *www.bitcoin.org*, 1-9.

Saviotti, P. P., & Metcalfe, J. S. (1984). A Theoretical approach to the construction of technological output indicators. *Research Policy 13*, 141-151.

Tapscott, D., & Tapscott, A. (2017). *Realizing the Potentail of Blockchain.* Geneva: World Economic Forum.

Acknowledgements

It is a pleasure to thank those who made this thesis possible, without them, it really was not possible. I would like to thank Professor B.M Sadowski for his guidance and advice during the research process. Additionally, I would like to thank the second and third assessors, Professor G.M. Duysters and Professor Z.O. Nomaler for their critical feedback.

I am really indebted and would like to thank all members of Rabobank's Blockchain Acceleration Lab for their countless inspiring sessions, discussions and enthusiasm during my research. In particular, I want to thank Djuri Baars for his guidance and patience during the process; he provided much valuable input for the research. Additionally, I would like to thank my fellow interns, Kim Hagelaars & Nick van Nispen who provided me support and lots of fun at the office.

I would like to thank Pascal van Hecke for providing me a ticket for the largest Ethereum developers' conference in Paris this year. It provided lots of insight and contacts used during the research. In addition, I would like to thank Bart Roorda for providing me a podium to present and validate my research findings during the Blockchain Innovation week in The Hague. My gratitude goes out to all interviewees that provided me many new insights during the research. In addition, I would like to thank all members of Techruption that were attending the TCB meetings; these meeting provided me helpful insights regarding the challenges of blockchain technology.

Finally, I would like to thank all my friends and family who helped and supported me during the process.

List of abbreviations

Abbreviation:	Stands for:	Chapter:
ASIC	Application-Specific Integrated Circuit	5.1.1
BAL	Blockchain Acceleration Lab	1.3
BIP(s)	Bitcoin Improvement Proposal(s)	5.1
BTC	Bitcoin Cryptocurrency	5.1.2
CBC	Correct By Construction	5.2.4
CCL	Cardano Computation Layer	5.3.1
CP(s)	Complementary Protocol(s)	4.2.2
CPCT	Cost Per Confirmed Transaction	5.1.2
CSL	Cardano Settlement Layer	5.3.1
DAC(s)	Decentralized Autonomous Corporations	5.2
DAO(s)	Decentralized Autonomous Organisation(s)	5.2
Dapps	Distributed Applications	5.2
DPoS	Delegated Proof Of Stake	5.3.1
EIP(s)	Ethereum Improvement Proposal(s)	5.2
ERCs	Ethereum Request For Comments	5.2.2
ETH	Ether Cryptocurrency	5.2.2
EVM	Ethereum Virtual Machine	4.2.1
FFG	Friendly Finality Gadget	5.2.4
GDPR	General Data Protection Regulation	4.1.2
ICOs	Initial Coin Offerings	5.2.2
IDC(s)	Internal Design Consideration(s)	4.2.1
IOHK	Input Output Hong Kong	5.3
ITRS	International Technology Roadmap For Semiconductors	2.1.4
KYC	Know Your Customer	1.3
MVP	Minimal Viable Product	5.1.4
PoC(s)	Proof Of Concept(s)	1.3
PoS	Proof Of Stake	2.2.4
PoW	Proof Of Work	2.2.4
RINA	Recursive Inter Network Architecture	5.3.4
SegWit	Segregated Witness	5.1.1
TCB	Techruption Consortium Blockchain	3.2
UTXO	Unspent Transaction Output	2.2

Table of Contents

List of Figures

List of Tables

1 Introduction

Blockchain technology and in broader terms distributed ledger technology (DLT), is a digital platform top trend in the Gartner hype cycle of 2017 (Panetta, 2017). Technology platforms, like Bitcoin and Ethereum are constantly in the news; however, the underlying technology blockchain is still in infancy. According to Tapscott & Tapscott (2017), the technology behind blockchain technology is pulling the world in a new era of openness, decentralization and global (economic) inclusion. Due to the high potential of the technology, many enterprises are looking how to deal with this new technology. A person or group with the pseudonym Satoshi Nakamoto who wrote a paper about the Bitcoin technology conceptualizes the first Blockchain application called Bitcoin. Nakamoto (2008) introduced "A purely peer-to-peer version of electronic cash that allows on-line payments to be sent directly from one party to another without going through a financial institution" (Nakamoto, 2008, p. 1). His paper described the first combination of individual technologies such as peer-to-peer and cryptography that together provides a truly peer-to-peer payment solution without the need of a trusted third party, called Bitcoin. Bitcoin was the first example of a digital currency relying on blockchain technology that could be used without the intervention of banks and or governments. Back then in 2008, the full potential was still unclear, however currently blockchain technology appears to become the foundation technology that leads to a fundamental change from trusting humans to trusting machines, and from centralized to decentralized control (Aste, Tasca , & Matteo, 2017). Blockchain technology is often described as the trusted economic layer of the Internet, something that was unthinkable before Nakamoto's paper introduction in 2008 (Swan, 2015). According to Tapscott and Tapscott (2017), blockchain technology is the foundation of the second-generation Internet, enabling to disrupt current business models and transforming industries. Arguably, the first generation of the Internet is perceptible as the information layer of the Internet where information acts as a public good. The second-generation Internet, which relies on blockchain technology, is perceptible as the value layer of the Internet where value as real asset can be exchanged without the use of a third party (Tapscott & Tapscott, 2017). The president of the ECB, Mario Draghi, argues in an interview: "We're very interested in this technology but it's not secure for central banking and therefore we need to look through it and investigate it more" (Francesco, 2018). In order to truly grasp the benefit and understand blockchain technology, this research qualifies the public blockchain technology characteristics. Additionally the current challenges for public blockchain technologies are described and this paper provides an overview of how some of these challenges will be addressed towards the near future by the open source technology communities. Furthermore, a conceptual model framework is introduced in the format of a characterisation guideline. Finally, the introduced conceptual model framework is validated by a multiple case study.

1.1 One universal framework to characterize blockchain technologies

Although much is already written about blockchain technology, there is no consensus about how technical characteristics of blockchain technologies should be described. Many different blockchain technologies use different classification frameworks and inconsistent names for proposed technologies. Furthermore, the International Organization for Standardization (ISO) is working on the so-called ISO/TC 307 for blockchain and DLTs, however currently under development and not completed yet (ISO, 2018). Although there is no uniform technology classification framework for blockchain technology available in literature, there are some approaches to classify different blockchains technologies. The upcoming chapters describe several types of characterising blockchain technologies.

1.1.1 Blockchain generations

In order to make the distinction of blockchain technologies a bit more convenient, Swan (2015) subdivided blockchain technologies in three different generations, which can be found in Table 1.1. Blockchain 1.0 is currency and stands for currency transfer, remittance and digital payment systems. Blockchain 2.0 is contracts and goes beyond simple cash transactions. The complete world economic market and financial applications are running on contracts and blockchain can autonomously check the requirements and execute the terms in those contracts without the need of a third party. Applications of Blockchain 2.0 are for example: stocks, bonds, futures, loans, mortgages, titles, smart property and

smart contracts. Blockchain 3.0 is blockchain applications, and goes beyond currency exchange, finance and markets and stands for decentralized applications (Swan, 2015). Decentralized applications or Dapps, from the outside look like today's Internet applications like Uber or Airbnb, however they do not require a third party to manage the user's information or to function and run in a decentralized manner to generate trust. The white paper of Ethereum mentions eight different examples of distributed applications: savings wallets, crop insurance, a decentralized data feed, smart multi-signature escrow, cloud computing, peer-to-peer gambling, prediction markets and on-chain decentralized marketplaces (Buterin, Ethereum White Paper, 2014).

Table 1.1 Blockchain technology generations. Derived from Swan (2015)

Blockchain generation:	Description:
1.0	Currency that stands for currency transfer, remittance and digital payments.
2.0	Contracts that goes beyond simple cash transactions.
3.0	Decentralized applications that go beyond currency exchange, finance and markets.

1.1.2 Public versus private blockchain solutions

There are two types of blockchain in terms of governance, public versus private blockchain solutions. The main difference between a private and a public blockchain is related to who is allowed to participate in the network, execute the consensus mechanism and have influence on the network (Jayachandran, 2017). In a public blockchain, anyone can join freely and participate in the network. According to CoinMarketCap (2018), Bitcoin is at the time of writing the most valuable public blockchain with a market capital of around 184 billion US dollar. A private blockchain network is managed by an authorized user or group of defined users who have authority to manage the network (Greenwood, Hillard, Harper, & Williams, 2016). The 'public versus private' blockchain definitions are often confused with 'permissionless versus permissioned' blockchains in literature. Therefore, this research introduces the different blockchain type definitions in chapter 2.2.2.

1.2 Challenges in blockchain technologies

Although Blockchain Technology is currently at the top of Gartner's hype cycle, the technology is not yet matured optimally, and feasibility studies are required before large-scale business implementation is possible (Wang, Chen, & Xu, 2016). Some people argue that blockchain technology is currently overhyped, since the technology has multiple limitations and is inappropriate for many digital transactions (Bauerle, 2018). Blockchain technologies are complex in multiple disciplines and require a divergent mind-set for people who work with it (Sit, 2018). Furthermore, public blockchain technologies have several challenges in practice that have to be solved before the technology can mature. Four challenges that are often described in literature are scalability, trust, privacy and energy consumption. The upcoming subchapters briefly explain these challenges.

1.2.1 Scalability

Current public blockchain technologies show multiple scalability issues. For example, the Dapp called 'CryptoKitties' that was launched on the 28th of November 2018 on the Ethereum platform (CryptoKitties, 2017). Due to mass adoption and viral marketing, CryptoKitties became popular in December 2017 and the Dapp processed over twelve million dollars' worth of CryptoKitties transactions (Young, 2017). This high popularity let towards a congestion crisis on Ethereum. Multiple Ethereum users were complaining about congestion, which means that people had to wait hours or sometimes-even days for their transactions to validate, or pay a much higher transaction fee (BCC, 2017). The current version of Ethereum is able to process on average 20 transactions per second and, in comparison to VISA that is capable of doing 56000 transactions per second, it needs a revolution to be competitive in terms of scalability (Vermeulen, 2017). However, the Visa network is centralized and VISA knows and trusts all the participating parties in its network and the Ethereum network is decentralized and does not know or trust all participants in the network. Another scalability issue is the

rapid growth in size of Blockchains. For example, the size of the Bitcoin blockchain is growing every block of transactions. On January 2018 the Bitcoin blockchain size already reached 150GB, and because the blockchain state of bitcoin is stored decentralized on all full nodes, this seems to be unsustainable (Blockchain.info, 2018). Currently there are solutions proposed by the blockchain communities to solve some of the scalability challenges like Raiden for Ethereum or Lightning for Bitcoin. Both solutions are currently tested and further elaborated in this research.

1.2.2 Trust

Blockchain is a technology for managing a lack of trust (Greenwood, Hillard, Harper, & Williams, 2016). The breakthrough innovation introduced by bitcoin is that participants can exchange value between each other, without knowing each other or trust each other (Atzori, 2015). This value is exchanged over a decentralized network of actors where the protocol defines the rules. Although Bitcoin and Ethereum are due to their open source nature controllable trustworthy, there were some issues where the trust in the network seems to be questionable. On the 17th of June 2016, Buterin (2016) who is the founder of Ethereum posted an update in the Ethereum blog where he explained that a decentralized autonomous organisation (DAO) running on the Ethereum platform was vulnerable. Due to this vulnerability, a user attacked the vulnerability and gained control over 3.6 million Ether that was worth roughly 50 million US dollar back then. The attacker was not able to withdrawal the 3.6 million Ether for another 28 days under the terms of the Ethereum contract. After much debate between the members of the DAO and the Ethereum community, a controversial fix was proposed after much debate. After a few days, the Ethereum community decided to hard fork the Ethereum blockchain. In block 1920000, an irregular state change transferred the money stored in the "Dark DAO" contract to the DAO recovery contract (Buterin, 2016). Because there was some debate whether to fork or not, the hard fork also led to a non-forked version Ethereum Classic in which the attack was not restored. Although this was not a trust issue in Ethereum, it was a bug in a 'smart contract' running on Ethereum and after the hard fork decision, some people argued that several tightly held assumptions emphasizing immutability of Ethereum where broken due to the decision, leading to a reduce of trust in the Ethereum platform (Spode, 2017).

1.2.3 Privacy

Although many people argue that Bitcoin is an anonymous payment network, Bitcoin is according to according to the Bitcoin foundation the most transparent payment network in the world (Bitcoin.org, 2018). Although the public addresses on Bitcoin are pseudonymous, Bitcoin consists of an immutable ledger where everybody is able to participate and which is transparent and openly accessible to everyone. This means that each transactions is linked to an electronic address and is made public. The identity of the user is not recognisable as long as the electronic address is not linked to a person. However, if someone links the address to a person's identity, the entire transaction history of that person is open and accessible. Security experts call this pseudonymous privacy (MIT Technology Review, 2017). Without privacy protocols, this openness and transparency can create issues for financial applications that are required to adhere to strict regulations (Baars, 2016). Simply encrypting the data and storing it in the blockchain is not sufficient, since the encrypted data is stored in the immutable blockchain and a potential attacker has an unlimited time opportunity to crack the encryption. Currently several privacy preserving techniques are available (Reitwiessner, 2016), however most solutions come with a trade-offs, like a higher capacity requirement from the network or the use of additional off-chain layers (Lightning Network, 2018).

1.2.4 Energy consumption

Several articles claim that the current energy consumption of the Bitcoin network is comparable to the energy consumption of the country Chile (Digiconomist, 2018). These energy consumption analyses are based on a single estimate of bitcoin's power consumption that is highly questionable (DiChristopher, 2017). However, there is no doubt that the consensus mechanism Proof of Work is energy inefficient since each Bitcoin miner around the world is trying to solve an identical cryptographic puzzle. Although above are serious challenges, currently much effort is made to solve these challenges

by the open source blockchain communities. This report describes the community efforts of several public blockchain technologies to solve the current issues. In order to do so, several community roadmaps are analysed and explained.

1.3 Rabobank's vision on blockchain

Blockchain Acceleration Lab (BAL) is Rabobank's centre of excellence regarding blockchain. Their first introduction with the technology was in 2014. Besides researching the technology parts of blockchain, they also identify new business models regarding blockchain technology. During their time, they already identified more than 200 interesting use cases for blockchain technology and built working prototypes like the sustainable pay-per-use project with a blockchain connected washing machine that pays using smart contracts on a blockchain or a boiler that could deliver energy back to the energy network and gets paid using blockchain technology. Furthermore, the team is working on a proof of concept (PoC) for know your customer (KYC) together with other external parties. Additionally, Rabobank has introduced a blockchain platform called 'we.trade' together with other European banks which already went live. Although current public blockchain solutions have several challenges and are in current format unfeasible for the strict regulation requirements for bank applications, Rabobank shows high interest in public blockchain solutions for the long run. Therefore, this research focusses mainly on public blockchain technologies. Furthermore, due to the high amount of identified use cases a conceptual model framework is introduced to characterise the design considerations of a public blockchain technology for a blockchain use case.

1.4 Research questions

Blockchain technology has attracted much attention in the last two years by promising large efficiency improvements for current regimes in many business sectors and 'cutting out the middlemen' (van Deventer, Brewster, & Everts, 2017). Many sectors are exploring use cases for blockchain technology to change their business ecosystems, but private blockchain platforms are often chosen as underlying technology because public blockchain technology platforms currently poses several challenges. The aim of this research is to address the current challenges of public blockchain technologies and describe the essential design consideration for public blockchain technologies specific for blockchain use cases. What are the current challenges for public blockchain solutions and how will these challenges be addressed in the near future? Understanding the process of innovation and the factors of technological change is crucial for the creation of a business strategy (Huenteler, Ossenbrink, Schmidt, & Hoffmann, 2016). The research is an interdisciplinary research relevant for both technologists and business enthusiast.

The main research question addressed by this research is *'How to qualify public permissionless blockchain technologies and why are these not wide-scale adopted for business use cases?'*

In order to answer the main research question, this thesis provides an answer to the following sub questions:

Sub question 1: *'How to characterise public permissionless blockchain technologies?'*

To address the main research question, it is useful to gain an understanding in public blockchain technologies. Chapter 2 elaborates on Sq1 and gives insights on several innovation theories useful as guiding lines for the characterisation of blockchain technologies.

Sub question 2: *'What are the essential design considerations in the selection of a public permissionless blockchain technology for business use cases?'*

The answer provided by Sq1 and Sq2 will form a conceptual model that is treated in chapter 4. Chapter 5 uses and validates this conceptual model with a multiple case study describing Bitcoin, Ethereum and Cardano.

Sub question 3: *'What are the current challenges within public permissionless blockchain technology platforms and how will the blockchain communities solve these challenges?'*

Sub question 3 will be answered in chapter 5 in the format of a case study. The answer of Sq3 will provide an overview of the current challenges and the proposed solutions of those challenges for some public blockchain platforms. The answers of the three sub questions are combined to provide an answer to the main research questions in the discussion section.

1.5 Research scope

Since there are many types of blockchain technology platforms, this section elaborates on the selection of public permissionless blockchain platforms. Public permissionless blockchains are defined in in chapter 2.2.2.

1.5.1 Public blockchain platform selection

Following Rabobank's interest for public permissionless blockchains and research time constraints, this research analyses three different blockchain platforms. These three are carefully selected, following the blockchain categorized way of thinking described by Swan (2015) combined with an analysis of the top ten cryptocurrencies with the largest market capital according to coinmarketcap.com (2018) at the time of writing.

Table 1.2 Top 10 cryptocurrencies based on their market capital on 17-01-18. Derived from CoinMarketCap (2018)

#	Public name	Name	Price per unit in USD	Market capital in million USD
1	**Bitcoin**	BTC	$ 10.228,70	$ 171.194 M
2	**Ethereum**	ETH	$ 873,82	$ 84.792 M
3	Ripple	XRP	$ 1,04	$ 40.231 M
4	Bitcoin Cash	BCH	$ 1.601,70	$ 27.095 M
5	**Cardano**	ADA	$ 0,50	$ 13.026 M
6	Litecoin	LTC	$ 162,68	$ 8.914 M
7	NEO	NEO	$ 111,63	$ 7.256 M
8	NEM	XEM	$ 0,79	$ 7.124 M
9	Stellar	XLM	$ 0,37	$ 6.642 M
10	IOTA	MIOTA	$ 2.26	$ 6.276 M

The longlist of top ten cryptocurrencies is transferred to a shortlist, which is highlighted in Table 1.2, containing the most interesting blockchain protocols for this research. Bitcoin is the foundation blockchain technology, blockchain 1.0 according to Swan (2015). Ethereum is "a next generation smart contract & decentralized application platform" (Buterin, Ethereum White Paper, 2014, p. 1) and is categorized as blockchain 2.0 by Swan (2015). The third blockchain picked for this research to analyse is Cardano. Cardano claims to be the next generation blockchain "completely evolved out of a scientific philosophy", promising to solve, sustainability, interoperability and scalability issues, that previous blockchain solutions tend to have (IOHK, 2018). Furthermore, all three protocols selected are completely build from scratch and not copies or forks from existing platforms. Ripple is not picked because of the limited use cases possible with XRP, and Bitcoin Cash is a fork of Bitcoin and Litecoin is bases on the Bitcoin source code.

1.6 Thesis structure

This thesis starts with a superficial introduction of blockchain technology, the current challenges and the research questions. The second chapter provides an overview of the innovation- and roadmap theories that are used as guideline for the characterisation of blockchain technologies. Additionally, chapter two elaborates on the taxonomy and technical details of distributed ledger technologies and a more in-depth literature analysis of blockchain technologies. The third chapter focusses on the research methodology. Furthermore, the fourth chapter describes the conceptual model. This model is later used

to perform a case study for three public blockchain solutions in the fifth chapter. Additionally, the conceptual model is validated with identified blockchain use cases in chapter six. Finally, the findings are discussed in chapter seven and the answers of the research questions are concluded in chapter eight.

2 Literature review

The literature review is divided in two subchapters. The first part describes the innovation theories that are applied in this research. The second part elaborates on the theories, taxonomy and the common definitions used to analyse blockchain technology.

This research builds upon the framework described by Saviotti and Metcalfe (1984) in order to give a clear characterisation of the services that blockchain as technology can deliver in relation to the technology characteristics of public blockchain technologies. The research uses an extended version of the innovation framework to describe the service and technological characteristics that blockchain as technology has. The innovation output of blockchain technology is hard to measure, since blockchain technology is still in infancy; therefore an analysis of roadmaps is performed to measure the technological change of three arguably important public blockchain technologies. During the research, the service and technology characterisation framework are composed using the innovation output obtained from a roadmap analysis plus a multiple-case studies.

2.1 Innovation theories

In order to describe the development of blockchain technologies, several innovation models are selected for this research and elaborated in this subsection. Since there is no single technology innovation framework that is capable of describing the complete innovation trajectory of blockchain technologies, a combination of frameworks is used to develop a conceptual model usable to characterise the technical and service characteristics of blockchain technology. Dosi (1982) has described a framework that studies technological change as paradigm or trajectory. A technological paradigm or trajectory sets the boundaries of a domain in which future technological change will take place.

2.1.1 Technology paradigms and technology trajectories

Dosi (1982) has proposed a model that describes discontinuous and continuous types of technological change. Discontinuous types of technological change are related to the emergence of a new technological paradigm. Continuous types of technological change are related to the continuously changing process of an existing technological paradigm. The rational for the model is to generate a way of thinking that argues, “Why a certain technological development emerges instead of others” (Dosi, 1982, p. 148). According to Huenteler et al. (2016), technological change of high-technology innovations often takes the format of long periods of incremental innovation along established technological trajectories, sometimes interrupted by the emergence of a new technological paradigm that is often introduced together with a radical innovation. Overarching to the study of technology paradigms and technology trajectories are design hierarchies. A design hierarchy can be described as “the technology-inherent hierarchy of design decisions” (Huenteler, Ossenbrink, Schmidt, & Hoffmann, 2016, p. 1195) and sets the boundaries for the trajectory of a technology. Technology trajectories can be analysed as cumulative processes where previous chosen trajectory paths acts as direction for future technological change (Dosi, 1982). Huenteler et al. (2016) suggest that the trajectory pathway of a technology is associated with its design hierarchy in two principal ways. Firstly, after the emergence of a new technological paradigm, the innovation agenda or roadmap of the technology is already set. This means that some general design decisions, like the individual components and some parts of the technology roadmap, are made at the emergence of a technological trajectory. Secondly, arguable important innovations are done earlier in the trajectory than less important innovations in the sub-systems of a technological trajectory. Studies have long argued about the existence of sequential patterns in the evolution of technology. In this context, ‘sequential’ means that innovations only apply in small fractions of the product architecture for a technology innovation. The order of this sequential nature of technological change can be related to two factors in the demand (technology push) and supply side (demand-pull) that both affect the evolution of technology (Huenteler, Ossenbrink, Schmidt, & Hoffmann, 2016). According to Dosi (1982), demand-pull is defined as technological trajectory where market forces act as main drivers for technological change. Technology push is defined as a

technological trajectory where technology as autonomous factor emerges from basic research, science or by brilliant individuals to address a yet unknown market need.

2.1.2 A framework to analyse the evolution of technology

Saviotti and Metcalfe (1984) have described a framework to analyse the evolution of a technology. The framework introduces two related sets of characteristics that can be used to characterise a product technology. The sets of characteristics can be separated in technical, process and service characteristics. These sets of characteristics form the basics of a framework to develop indicators to measure the output of technology. In order to develop innovation indicators, for example for blockchain technology, the innovation output of the technology should be unequivocally defined. The three sets of technical, process and service characteristics are made more specific by introducing two types of institutions. The first is the user institution that is mainly interested in the services delivered by a product and the economic costs coming with a product. The second is the producer institution that responds to the will of the user institution and supplies these services by a combination of technical characteristics. Both institutions can describe demand-pull or technology push trajectories or a combination of both. The separation of the two institutions suggests that a product can be described as two sets of characteristics and the relation of the two that are the service characteristics (Y_i), the technical characteristics (X_i) and a pattern of mapping that describes the relations between the service and technical characteristics. The interaction and the subsystems described by the services and technology characteristics is organized by the 'product architecture' (Huenteler, Ossenbrink, Schmidt, & Hoffmann, 2016). An overview of the framework described in this section is given in Figure 2.1.

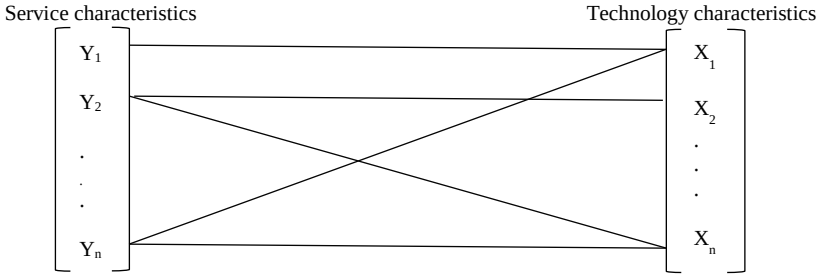


Figure 2.1 **A product architecture described as two sets of service and technological characteristics are interlinked by a pattern of mapping. Adapted from Huenteler et al. (2016).**

Dosi (1982) mentions continuous and discontinuous types of technological change. A discontinuous type of technological change leads to a considerable new design and a new paradigm of technology. After a discontinuous type of technological change occurs, the new design of technology will have a different set of technology characteristics (X_i), but a matching set of service characteristics (Y_i). Figure 2.2 describes the change process of the characteristics framework of a product during a discontinuous type of technological change. A continuous type of technological change will not lead to different technology characteristics, and only implement some incremental changes in the product architecture. The set of technology characteristics will generally stay equal.

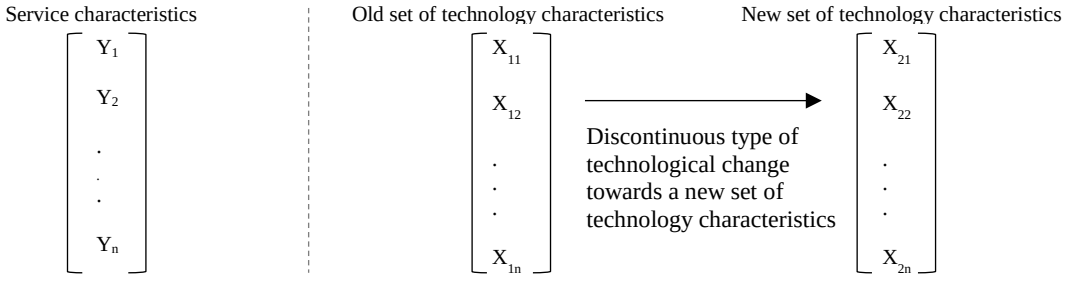


Figure 2.2 **A product described as two sets of characteristics (service and technology) including a paradigm shift towards a new set of technical characteristics**

Many modes of innovation lead to different technology characteristics for a technology. The visualization of technological change described in Figure 2.2 is an example of a discontinuous type of technological change. The next chapter will elaborate on the types of technological change that are described as the innovation types for service industries.

2.1.3 Innovation types for service industries

Gallouj & Weinstein (1997) have introduced a taxonomy how innovation processes can be interpreted in the service industries. The paper first elaborates on the service / technology characteristics framework described by Saviotti and Metcalfe (1984), which is described in chapter 2.1.2, and afterwards elaborates on the "modes and models of innovation". Gallouj & Weinstein introduce six different modes of innovation that are used in this paper to study technological change in blockchain solutions.

Radical innovation: The definition 'Radical innovation' points out the creation of a completely new product. The product architecture is entirely new and not known in that particular domain.

Improvement innovation: The definition 'improvement innovation' is interpreted as 'performance enhancing' innovation, where parts of the product architecture are improved, to improve the service characteristics of an innovation. There is no change in the product architecture, only some properties of the technology characteristics are improved to gain a performance increasement of the service characteristics.

Incremental innovation: Incremental innovation is somewhat comparable to improvement innovation however there is a slightly difference. Some changes in the product architecture are implemented and not improved.

Ad hoc innovation: Ad hoc innovation can be "defined in general terms as the interactive (social) construction of a solution to a particular problem posed by a given client" (Gallouj & Weinstein, 1997, p. 549). A technology can improve its service characteristics with a solution introduced by a client or application that uses the technology, and without changing the product architecture.

Recombinative innovation: Recombinative innovation, which is also called architectural innovation, describes an innovation where new combinations of different older solutions are combined into a new product. This kind of innovation builds upon old solutions and combines it towards a new product architecture.

Formalisation innovation: The various modes of innovation outlined above are based on variation within the product architecture, by adding, eliminating, improving, combining or splitting parts. The formalisation innovation model, describes finding the service characteristics, making them more specific and less hazy, and afterward putting in place the technical characteristic, whether tangible (e.g. equipment, software) or intangible (e.g. methods, organisations, toolboxes) technology characteristics. The formalisation model is sometimes compared with the recombinative model, although the formalisation innovation model clearly starts with ordering the service characteristics.

The six modes of innovation are used in this paper to describe different innovation processes and separate them.

2.1.4 Roadmap Analysis

Blockchain technology is still in infancy, and many enterprises, start-ups and governmental organizations are currently looking for potential blockchain use cases. Blockchain technology has several properties like decentralization and since blockchain technology is still in infancy, there is not enough quantitative data available about blockchain technology to perform a quantitative analysis like for example a patent analysis. In addition, blockchain technology can arguably be described as a service innovation, and service innovations have a 'fuzzy' nature of their output and therefore it is hard to detect

improvements or change in the technologies in traditional ways (Gallouj & Weinstein, 1997). Above challenges and characteristics, make it hard to measure the innovation output of Blockchain technologies.

In order to qualify the technology innovation process of blockchain technologies, this paper uses among other things a roadmapping analysis to measure the innovation output of blockchain technology. Although there is no general analysis method for roadmaps described in literature, the paper uses knowledge derived from technology roadmapping papers that describe the process and taxonomy of creating roadmapping for current companies or industries.

A roadmap is defined as "an extended look at the future of a chosen field of inquiry composed from a collective knowledge and imagination of the brightest drivers of change in that field" (Kostoff & Schaller, 2001, p. 132). Roadmaps provide a structured overview of shared visions, stimulate innovation and monitor the progress made by an innovation. A roadmap provides a common consensus view or vision toward the future of a technological trajectory. According to Reuver et al. (Reuver, Bouwman, & Haaker, 2013), the process of roadmapping itself is considered more useful than the result of the roadmap. The process of roadmapping will improve communication between actors, and enable companies to focus their long-term planning and priorities. This seems like an interesting approach for open source communities to reach consensus about their research effort. There are two well-known roadmap perspectives described in literature, a multi-organizational and a company perspective (Phaal, Farrukh, & Probert, 2004). From the multi-organizational perspective, one of the most well-known roadmap cooperation's is the *International Technology Roadmap for Semiconductors* (ITRS). This corporation provides technology roadmaps for the semiconductors industry. The rational of the organisation is to provide a 15-year horizon for the semiconductor industry to guide the efforts of companies, research organisations and governments to improve their R&D investments and address areas that need breakthrough innovations. Hence, the roadmap provided by the ITRS is set up to specify the technical capabilities required from the industry in order to follow Moore's law (Allan, et al., 2002). The roadmap created by ITRS is a multi-organizational roadmap describing the shared interest and consensus vision for the future of a complete industry. The other way of roadmapping is from a company perspective. A roadmap from a company perspective describes technology developments in relation with business planning and the influence of new technology and market developments (Phaal, Farrukh, & Probert, 2004).

2.2 Blockchain Technology

Satoshi Nakamoto (2008) introduced the first application of blockchain, called Bitcoin. Bitcoin is introduced as "electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party" (Nakamoto, 2008, p. 1). Baars (2016) defines blockchain as "A chain of blocks, where each block contains unchangeable records". A blockchain serves as a distributed ledger where all transactions are stored in blocks and each generated block contains references towards previous blocks in the form of a hash. After a block is included in the blockchain and the there is consensus over the included block, it will become economically unfeasible to change transactions stored in that block. A blockchain acts as an append-only immutable ledger. Blockchain technology can be used as distributed ledger technology allowing transactions taking place in a distributed and trusted manner.

The blockchain technology is the underlying technology enabling cryptocurrencies like bitcoin. In the case of Bitcoin, the records in the ledger represents an amount of unspent *bitcoin cryptocurrency* (BTC) assigned to a public key. The blockchain acts as an open append-only ledger where everyone is able to observe and validate all transactions. Each transaction is secured by public key cryptography (Baars, 2016). In order to conduct a transaction, the possession of a key pair, consisting of a public and a private key, is required. Each validator of transactions has access to the blockchain that contains a list of all unspent funds. After a transaction has happened, the corresponding entry changes from unspent to spent. Therefore, a bitcoin is only spendable once, and blockchain technologies solve the double spending problem (Anderson, Holz, Ponomarev, Rimba, & Weber, 2016).

Zheng et al. (2017) characterizes public blockchain technologies into four key characteristics. The pseudo-anonymity definition is described by Yaga et al. (2018).

- *Decentralization*: Contradictory to decentralization is the conventional centralized transaction system. Trusted third parties, i.e. Banks, validate transactions on centralized servers. Public blockchain platforms enable direct transactions with the requirement of trusted third parties. Blockchains use consensus mechanisms in order to maintain data consistency over the distributed network.
- *Persistency*: Blockchains are restricted to rules that are defined by their protocols. A network of validators or miners validates transactions. Cryptoeconomics incentives make it economically infeasible to manipulate transactions that are included in the blockchain. Cryptoeconomics is elaborated in chapter 2.2.5.
- *Pseudo-anonymity*: Everyone is able to interact with a public permissionless blockchain by a generated key pair that does not reveal the identity of the person behind the public key. The public key is as the name suggests public and everyone is able to see its transaction history of that key. The private key is as the name suggests private, and the combination of both keys provides spending rights to the corresponding ledger entries.
- *Auditability*: Everyone can validate the complete chain of blocks and the full audit log of transactions. Bitcoin uses the user *unspent transaction output* (UTXO) model as audit log. Each transaction has to refer to a previous unspent output of a certain account. If a transaction has occurred, the unspent transaction output of an account changes from unspent to spent.

Because blockchain technology is a part of the umbrella term DLTs, this chapter first elaborates on DLTs. Secondly, the differentiation between a public permissionless, a public permissioned and a private permissioned blockchain is given. Thirdly, a more in-depth technology explanation is given describing a blockchain as a chain of blocks and consensus mechanism are elaborated. The latter terms describe the common knowledge of blockchain technology. In order to provide a deeper and differentiating understanding of blockchain technology the relatively novel term ‘cryptonomics’ is explained, describing some economics of blockchain technology. Additionally, a method of evaluating the value of blockchain platforms is treated, and a philosophical explanation of blockchain as a social technology is described. Both are placed in Appendix III & Appendix IV.

2.2.1 Distributed ledger technologies

Ledgers are used in many areas of commerce since ancient times to record things like assets, money and property (Greenwood, Hillard, Harper, & Williams, 2016). During this time, ledgers where written on clay tablets, vellum and eventually paper. The only breakthrough innovation for ledgers was made by computerisation, from paper to bits and bytes. Alongside with this digitization of ledgers was the introduction of distributed ledgers. A distributed ledger is in essentials an asset database that is shared in a distributed way across multiple sites or geographical locations. Each ledger state update made by an actor should be updated with all the ledgers in network within minutes or in some cases within seconds. The integrity of the ledger is obtained using key pairs and signatures to manage access restrictions of participants regarding a specific set of rules defined in the protocol. (Walport, 2016).

A ‘Ledger’ is described as a collection of transactions. Since the digital age, ledgers have been stored digitally, and sometimes ledgers are stored by ‘trusted third party’ on behalf of a group of users (Yaga, Mell, Roby, & Scarfone, 2018). Greenwood et al. (2016) describe three ways of maintaining a ledger resulting in central, replicated and distributed ledgers (Table 2.1).

Table 2.1 **Three ways of maintaining a digital ledger, derived from Greenwood et al. (2016).**

		
A centralized ledger is maintained by a single central authority. The current state of a centralized ledger is the 'ledger of record' that is available from the central authority. Access management to the ledger assures ledger identity and integrity. If the centralized party is not properly backing up the data ledger, the data could be lost or destroyed and therefore each user has to trust the integrity of the owner.	**A replicated ledger** is maintained by a single central authority. The current state of the ledger is everything that is in the 'ledger of record'. Other actors must ask the central authority if they want to use the data in the ledger. Other actors can synchronize their copy with the central ledger to be able to access it locally; however, they are responsible for keeping their version of the ledger up-to-date. Access management to the ledger assures ledger identity and integrity.	**A distributed ledger** is maintained by a group of peers within a peer-to-peer network. The current state of the ledger is represented as the state where all peer's agree and reach consensus about. Other actors can retrieve a copy of the ledger from any of the peers within the peer-to-peer network. Furthermore, other actors can present their new records to the distributed ledger network. Ledger integrity is assured by the consensus mechanism.

The advantage of a distributed ledger is that there is no reliance in a centralized party and therefore there is no central point of failure if one node is congested or attacked. With no single authority or organisation being responsible for the integrity of the ledger, all peers have to reach consensus about the state of the ledger. The way of reaching consensus depends on the level of trust network participants have in each other. Consensus mechanisms are further elaborated in chapter 2.2.4.

The three types of maintaining a ledger can also be compared with the different types of network topologies. Yaga et al. (2018) have recently described three types of networks topologies. The comparison is made in Table 2.2.

Table 2.2 **Overview of the three types of networking topologies, derived from Yaga et al. (2018).**

		
A centralized network topology is network configuration where all nodes have to communicate with a single central hub. If this hub fails, the whole network falls apart. There is one single point of attack in to shut down the whole network.	**A decentralized network topology** is a network configuration where multiple authorities work as a centralized hub. If those hubs fail due to an attack, some nodes will be excluded from the network. There are single points of attack to exclude parts of the network.	**A distributed network topology** is a network configuration where each node can communicate with one another node, without the reliance of a single party, since there are multiple pathways to communicate. The loss of a single node will not harm the network, and this type of network is known as peer-to-peer. There is no single point of attack in the network and there is no difference between a centre or endpoint node.

Besides the three types of network topologies, a distinction could be made between permissioned and permissionless ledgers. Yaga et al. (2018) clarified the difference between permissioned and permissionless distributed ledgers. The difference between the two ledger types is determined by the access restrictions of the validation process. Bitcoin is as a permissionless ledger and everyone is able to participate in the validation process, i.e. become a miner. In a permissionless ledger, all participants of the ledger are allowed to participate in the consensus process and together maintain integrity about the state of the ledger. Within a permissioned ledger, the consensus process is restricted to a set of authorized participants. Since parties in a permissioned ledger know each other, involved parties share a higher level of trust and the consensus mechanism can be less computationally complex. Therefore, permissioned ledgers can reach high transaction speeds than permissionless ledgers.

2.2.2 Public, consortium and private blockchain types

Zheng et al (2017) and Buterin (2015) categorize current blockchains into three types: public, private and consortium blockchains. Both describe a public blockchain as a permissionless ledger where all records, also called the 'state' of the chain, are open and accessible and each stakeholder is allowed to participate in the network. Additionally they define a private blockchain as a blockchain of one organisation with a permissioned consensus mechanism. A Consortium blockchain is a mix of both worlds, and is a blockchain where consensus is reached by a predefined set of nodes. Zheng et al. (2017) identified six taxonomy properties to describe the difference between a public, a consortium and a private blockchain solution (Table 2.3).

Table 2.3 Overview of three types of blockchain systems versus the design properties. Derived from Zheng et al (2017) and Buterin (2015)

	public blockchain:	**consortium blockchain:**	**private blockchain:**
Consensus determination	Determined by consensus mechanism	Selected set of nodes	One organisation or person
Read permission	Public	Public or restricted	Public or restricted
Immutability	Depends on the consensus mechanism. Consensus mechanisms are treated in chapter 2.2.4.		
Efficiency	Lower	Higher	Higher
Centralized	Considered "fully decentralized"	Considered "partially decentralized"	Centralized to one organization or person
Consensus process	Permissionless	Permissioned	Permissioned

Since there is much overlap and discussion about the above public, private, permissioned and permissionless blockchains types, this research builds on three type definitions for blockchain technologies that are used during the research:

- *Public permissionless*: everybody is allowed to access and participate in the blockchain, and everyone is allowed to participate in the consensus mechanism. Examples of this type are Bitcoin and Ethereum.
- *Public permissioned*: everybody is allowed to access and participate in the blockchain, however participation to the consensus mechanism is restricted. Examples of this type are Ripple and Hyperledger Indy.
- *Private permissioned:* The network is only accessable for a authorized group of users, and participation to the consensus mechanism is also restricted.

This research uses the "*public permissionless"* blockchain type definition to define the scope of the research and the research question. In this definition, public versus private stand for who is allowed to access and participate in the blockchain, and permissionless versus permissioned stands for the access restrictions for the consensus mechanism. For a public permissionless blockchain, everybody is allowed to access and participate in the blockchain, and everyone is allowed to participate in the consensus mechanism. These definitions are validated in multiple interviews and meetings with experts.

2.2.3 Chain of blocks

The notion of blockchain is best described as "a continuous sequence of blocks" (Baars, 2016). Blockchain is structered as a continious sequence of blocks, that all combined hold a complete list of transactions like a conventional distributed ledger. The difference with a conventional distributed ledger is that in a blockchain the transactions are ordered into blocks. Figure 2.3 shows a schematic overview of a blockchain as a continious sequence of blocks. Each block refers to the previous block with the 'parent block hash' and the chain ends at the start at block 0, which is called the 'genenis block'. "A genesis block is the unmined, deliberately created, very first block in a blokchain and has no predecessors, i.e. no parent block" (Pfeffer, 2017). Aditionally the genesis block contains protocol defining the rules that the blocks have to follow.

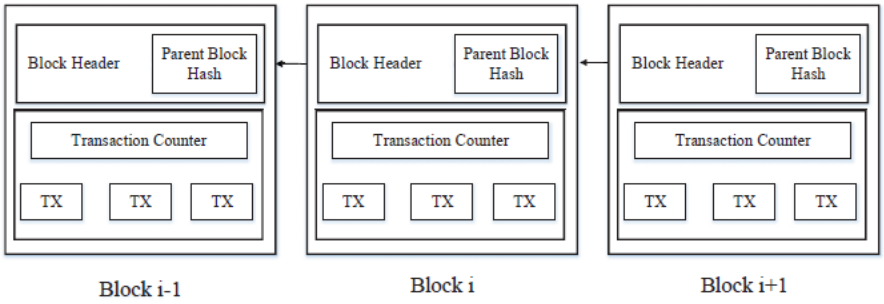


Figure 2.3 An example of a blockchain consisting of a continuous sequence of blocks. Adapted from Zheng et al. (2017).

Each block contains a block header and a block body that is shown in Figure 2.4. According to Zheng et al. (2017), the block header in the bitcoin blockchain includes:

- *The block version:* indicates the protocol version of the block including the block validation rules of the blockchain.
- *The merkle tree root hash*: contains the hash tree information in SHA256 format of all transactions within the block. Merkle trees and hashes are covered below.
- *Timestamp*: the timestamp when the miner has started hashing the header of the block in universal time.
- *nBits*: is an encoded version of the target treshhold this block's header hash must be less than or equal to.
- *Nonce*: A random number, miners could change to modify the header hash, in order to produce a hash lower than the treshold.
- *Parent block hash*: the SHA256 hash of the previous mined blockheader.

Besides the block header, the bitcoin blockchain also contains the block body. The block body contains the transaction counter and the list of transactions stored by the block.

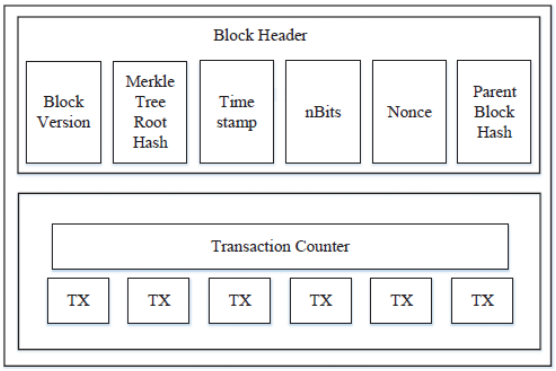


Figure 2.4 An example of a Blockchain block with its internal structure. Adapted from Zheng et al. (2017).

There are some differences in how the blocks are implemented in Bitcoin and Ethereum. In Ethereum, the block headers also contain the ommersHash, which is the hash of the orphan blocks (Wood, 2014). An orphan block is another child of a blocks ancestor. In the bitcoin blockchain, this block would be removed since it will be indicated as an orphan block, and these are not allowed by the bitcoin protocol. In the Ethereum protocol, orphan blocks are accepted since targeted block release times in Ethereum are roughly ~12 seconds per block in comparison to ~10 minutes for Bitcoin. Due to this short block time, network latency becomes a bigger issue. Orphan blocks are accepted within Ethereum to compensate miners that find duplicated blocks unintentionally. The orphan is than implemented as uncle block in the chain.

Hashing

Hashing is a one-way mathematical operation that compiles a given input of original data into a summarized fixed-length binary sequence, which is called a digest (Baars, 2016). Because hashing works only in one direction, it is impossible to retrieve the original data from the hash digest.

Merkle tree root hash

In most blockchain technologies, a Merkle tree secures the transactions within a block. Figure 2.5 contains a schematic overview of the Merkle Tree containing eight transactions.

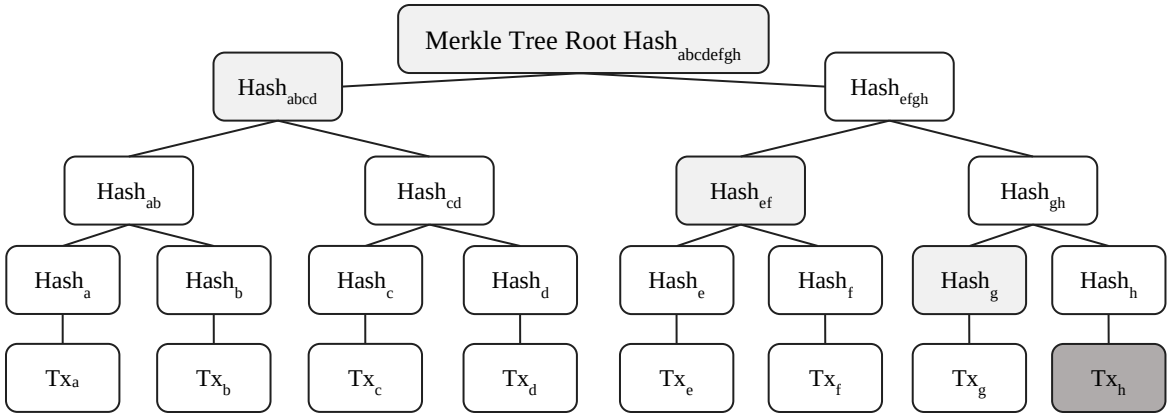


Figure 2.5 Overview of schematic Merkle tree of bitcoin containing eight transactions

The Merkle tree is calculated bottom up, containing all transactions and the block header data, and the Merkle tree root hash is stored in the block. The Merkle tree enables single transaction validation without downloading the complete block. In Figure 2.5, Tx_h can be validated with the Merkle tree root hash, $Hash_{abcd}$, $Hash_{ef}$, and $Hash_g$ and this drastically limits the bandwidth requirements of a network. According to Ray (2017), Merkle trees provide three major benefits: first, they provide a simple way to proof the integrity and validity of the records or transactions. Secondly, storing a Merkle tree is more efficient that storing a complete database. Thirdly, creating Merkle proofs and the management of the trees requires small amounts of bandwidth and computation power and this enables, limited in computation power, light clients to validate single transactions without verifying the complete chain (Buterin, Introduction to Cryptoeconomics, 2017). The fact that each block contains the Merkle Tree Root Hash of the previous block creates the chain of blocks. The Merkle Tree Root Hash of the most recent block arguably contains the hash of the whole chain. Therefore, the Merkle tree root hashes will not correspond if a single transaction somewhere in the chain is changed.

Conflicts in the chain: Transaction finality and forks

Because a blockchain is literally formed as a chain of blocks, there is a possibility that the chain splits at some point. This is called a fork. When a fork occurs, two blockchains are created with a shared genesis block that are identical until the forking point, and afterward exist both exclusively in parallel creating two separate networks unless one of the chains in abandoned (Danova, 2015). A fork can occur unintentionally due to issues like for example network latency, i.e. multiple nodes behold different states of the blockchain, or intentionally due to issues like a disagreement in protocol rule changes or a malicious attacker creating an invalid block. These forks create an issue if a blockchain deals with a digital currency, money may be spent in one block, and unspent in the conflicting block, the well-known double spending problem. However, conflicts like this in blockchain are usually quickly resolved, and the longest chain will eventually be considered as the ‘official’ blockchain (Yaga, Mell, Roby, & Scarfone, 2018). Figure 2.6 visualizes a conflict in a blockchain between two blocks at block height #4. One of the chains contains a wrong transaction in block #4 and that chain is automatically abandoned after the correct chain is longer. Sometimes, if a conflict happened unintentionally both conflicting blocks are not wrong, because they were created due to information asymmetry. In Ethereum, the

conflicting blocks are accepted in the chain as ‘uncle blocks’ and therefore creators are also receiving a part of the block reward (Zheng, Xie, & Dai, 2017).

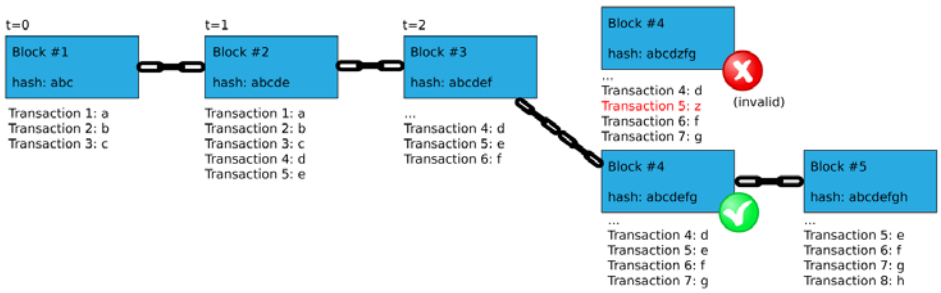


Figure 2.6 Blockchain as a ‘chain of blocks’ with conflicting block #4. Adapted from Baars (2016)

Blockchain forks can also occur with good intentions. Yaga et al. (2018) describe the process of forking as an update of technology. Changes to the blockchain protocol are extremely difficult to carry out since blockchain platforms contain many users distributed around the world all with different governance incentives. Yaga et al. (2018) describe two types of forks, a soft and hard fork. A soft fork is a change in the blockchain protocol that will not exclude users that do not adopt the change, i.e. update to the last version. Since nodes that run the old software still accept the new blocks, a soft fork is backwards compatible and only requires the majority of nodes to upgrade to the new protocol rules to make the fork successful. A hard fork is a change in the blockchain protocol that will exclude users from doing transactions who not update their software to the new hard fork requirements. Any change to the block structure, such as a change in the consensus mechanism or in the hashing algorithm requires a hard fork. A famous example of a hard fork is the past Ethereum DAO hard fork, which is described in chapter 1.2.2.

Another conflicting issue of blockchain as ‘a chain of blocks’ is that current large blockchain platforms do not offer a 100% truly transaction finality. Buterin (On Settlement Finality, 2016) describes “finality” as the property: “once an operation is completed, that the operation is completed for good, and there is no way that the system can ever go back and revert that operation”. It is important to notice that there is no system in the world that offers 100% truly transaction settlement finality. In the centralized ledger world this is an issue because a paper ledger can be burned or a drawn ‘1’ can be made look like a ‘9‘. Furthermore, a malicious attacker can attack each centralized digital ledger. Although the chance is small, there is always a chance that data is lost or will be changed. In blockchain platforms, the consensus mechanism, the law and economic incentives are properties of blockchain platforms that influence the settlement finality of the system (Buterin, On Settlement Finality, 2016). In Bitcoin, so far there have been several instances where transaction finality was reversed after a period. Three of them are:

- In 2010, a hacker was able to create 186 billion BTC by using an overflow bug in the protocol. The bug was fixed within 5 hours by a soft fork change to the consensus mechanism and the transaction of 186 billion BTC did not exits after the chain was forked (Bitcoin Wiki, 2016).
- In 2013, the bitcoin blockchain was forked due to a bug existing in one version of the software but not the other version. This bug led to a fork. The split of the chain was solved after 6 hours (Buterin, Bitcoin Network Shaken by Blockhain Fork, 2013).
- In 2015, six blocks in the bitcoin blocks contained invalid transactions in the Bitcoin blockchain after a mining pool was mining invalid blocks without verifying them. (Bitcoin.org, 2015)

According to Buterin (On Settlement Finality, 2016), two of above errors emerged from software bugs and one of them because of a fault in the economic incentive model in bitcoin.

2.2.4 Consensus mechanisms

Consensus is the process of building mutual agreement between groups of mutually distrusting users (Hyperledger Sawtooth, 2018). This process is complex to apply in computer networks since the byzantine generals' problem is a large problem for peer-to-peer networks. A solution of this problem is proposed by the *Proof of Work* (PoW) mechanism in Bitcoin. After the introduction of PoW, multiple blockchain platforms introduced many alternative consensus mechanisms to enable a group of mutually distrusting users to work together (Yaga, Mell, Roby, & Scarfone, 2018). Another issue that Peer-to-peer networks generally have are the so-called 'Sybil attacks' (Aumasson & Jovanovic, 2016). In a Sybil attack, the attacker creates a large amount of pseudonymous identities, to gain a large influence in the network. Public permissionless blockchains require a mechanism to prevent them from this type of attack, and this system is the consensus mechanism (Aumasson & Jovanovic, 2016).

If a user joins a public blockchain platform, the user agrees to the initial state and the protocol describing all the rules recorded in the genesis block. Each blockchain consists of a genesis block and all changes in the state have to be published in the blocks after the genesis block. Furthermore, each block has to be valid and each user should be able to check the validity of the blockchain. Yaga et al. (2018), argues that the following properties are in place:

- If users participate in the network, they agree to the initial state described in the genesis block.
- Users have to agree with the consensus mechanism about set of rules describing who is allowed to add blocks to the chain.
- Each block is linked to the parent block using a hash, except for the genesis block.
- All users can verify every block and thus can verify the complete state and each transaction in the chain.

All above properties are described in the protocol. One key aspect of how public permissionless blockchain works is that no trusted third party is required to determine the state of the ledger, and everyone can verify the complete state and the integrity of the chain. In order to add a block to the blockchain, all users have to reach a common agreement, in other words consensus, over time. A disagreement is permitted only for a short amount of time. The method of reaching consensus must be trustworthy even if some malicious user tries to gain control over the blockchain (Yaga, Mell, Roby, & Scarfone, 2018). Not each user of a public permissionless blockchain is obligated to take part in the consensus process, since users can trust the integrity of the network (Zheng, Xie, & Dai, 2017). This chapter elaborates about the two different mechanism of reaching consensus for public permissionless blockchains. Three other consensus mechanism and a general comparison are placed in Appendix I.

Proof of Work (PoW)

The PoW consensus mechanism is also called the Nakamoto consensus mechanism (Hyperledger Sawtooth, 2018). In this mechanism, the miner is assigned to be a temporary dictator allowed to publish the next block by solving a computationally complex puzzle. The solution of the puzzle will become the proof that a certain actor has performed an amount of work (Yaga, Mell, Roby, & Scarfone, 2018) and the proof that they have access to a certain amount of computational power (Buterin, Introduction to Cryptoeconomics, 2017). The puzzle is designed to be very hard to solve and very easy to verify just as Sudoku. Examples of PoW algorithms are Bitcoin's PoW that uses SHA-256 cryptography and Ethereum Ethash that uses SHA-3 cryptography. The general idea of PoW is that the amount of computation power a miner has relates to the chance of mining a block. This leads to a distributed level of control where no single actor is able to gain control over the blockchain. However, there are multiple criticisms found in literature towards the PoW consensus mechanism. Firstly, PoW burns massive amounts of energy since each miner in the world is trying to solve an identical puzzle. The miner that solves the puzzle first is allowed to publish the block and collect the rewards. (Aumasson & Jovanovic, 2016). Secondly, the PoW consensus model assumes the 'honest majority model' that states that 51% of the networks acts honest and additionally the PoW consensus model assumes the uncoordinated choice model that states that actors all act individual and uncoordinated (Buterin, Introduction to

Cryptoeconomics, 2017). The uncoordinated choice model assumption is violated since the introduction of mining pools (Wang K. , 2017). A mining pool is a coordinated action by a group of miners in the form of a pool. Specially, because the rewards of PoW are distributed, mining pools stabilize the earnings for a miner. Within a mining pool, all miners solve a part of the puzzle, and together they share the revenue. According to blockchain.info (Blockchain.info, 2018), the current largest mining pool is BTC.com and this pool manages about 25.7 percent of total computer power of bitcoin mining. This leads to the third critical point of PoW that is Selfish Mining. The idea behind selfish mining is to keep discovered blocks private, and thereby intentionally forking the chain. The honest miners continue to mine blocks on the public chain, will the selfish miner mines their own chain (Eyal & Sirer, 2014). If the computation power of the selfish mining is higher than 25% of the total computational power of the network, the selfish mined private chain will eventually contain more blocks than the public chain (Buterin, Introduction to Cryptoeconomics, 2017). At this moment, the private chain is provided to the network. The longer chain will be selected as the 'valid' chain, and the 'honest' chain will be rejected and all block rewards will go to the selfish miner. Overall, the criticisms regarding PoW in literature are energy consumption, selfish mining and the potential violation of honest majority and uncoordinated choice assumptions.

Proof of Stake (PoS)

The main idea behind PoS is that the more stake a user has in the system, the more likely a user want the system to succeed. "Stake is an amount of cryptocurrency that the user has invested into the system, either by locking it via a special transaction type, or by sending it to a specific address; the amount of staked cryptocurrency is no longer able to spend" (Yaga, Mell, Roby, & Scarfone, 2018, p. 29). The PoS mechanism is a generalization of the PoW mechanism, although the miners are identified as validators and the Proof of solving a puzzle is changed to the proof the ownership of an amount of stake in the system (Zheng, Xie, & Dai, 2017). The PoS mechanism of reaching consensus does not require a resource intensive generated PoW. Therefore, PoS is a much more effective and energy efficient mechanism of reaching consensus and Ethereum is planning to move from its PoW implementation Ethash towards a PoS implementation called Casper (Zheng, Xie, & Dai, 2017).

Yaga et al. (2018) identifies two types of PoS mechanism: the so-called Chain-based PoS and the so-called Byzantine Fault Tolerance PoS. In chain-based PoS, The likelihood a user has to be picked as validator of a new block is defined by the ratio of their stake to the complete amount of stake staked in a blockchain platform (Yaga, Mell, Roby, & Scarfone, 2018). If a user is in possession of 42% of the stake staked in a blockchain solution, the user is picked as validator for 42% of the blocks. In Byzantine Fault Tolerance PoS, there is some sort of complexity added. For each new block, the system will select multiple validators based on their staked stake as potential validators for the next block. Then each potential validator is asked to create a block, and all potential validators will vote afterwards which block will be implemented in the blockchain (Yaga, Mell, Roby, & Scarfone, 2018). Additionally, there are multiple types of PoS mechanism, i.e. based on the age of cryptocurrency like Peercoin and many others (Zheng, Xie, & Dai, 2017).

There are criticisms about the PoS mechanism. Firstly, the "rich" in PoS systems can easily stack more stake into the system, earning themselves more returns, and gain more control over the system in theory (Yaga, Mell, Roby, & Scarfone, 2018). Secondly, there is nothing at stake in the event of a fork. It does not matter whether the fork is intentional or not but there is no stake within the chain that does not win. Therefore, each validator in theory is incentivized to validate on both chains after a fork since there are no extra costs. In this case, an attacker can buy their other digital goods on an exchange, and after the exchange transaction has happened, the attacker could fork the chain from the point before the exchange of tokens took place. Because every validator is mining on both chains, the fork has a chance to win (Buterin, Ethereum Wiki / Problems, 2017). Although these are all serious concerns, much work is currently done to create hybrid forms of consensus mechanism such as Casper (Buterin & Griffith, Casper the Friendly Finality Gadget, 2017).

2.2.5 The economics of public permissionless blockchains: Cryptoeconomics

Blockchain platforms use different consensus mechanism to maintain integrity in the chain. Consensus mechanisms provide an answer to the byzantine generals' problem in computer science (Wang K. , 2017). "A reliable computer system must be able to cope with the failure of one or more of its components. A failed component may exhibit a type of behaviour that is often overlooked--namely, sending conflicting information to different parts of the system. The problem of coping with this type of failure is expressed abstractly as the Byzantine Generals Problem" (Lamport, Shostak, & Pease, 1982, p. 382). It is difficult for a distributed network to deal with failing or malicious actors, because the network must reach consensus about the exclusion of those untrusted actors. Buterin (Introduction to Cryptoeconomics, 2017) introduces the term "cryptoeconomics" as design methodology to design a robust mechanism of reaching consensus across a distributed network. Buterin describes Cryptoeconomics as a combination of cryptography and economic incentives that together set the design decisions for a consensus mechanism. Furthermore, Buterin claims that blockchain is a unique technology that combines cryptography and economics. Cryptography allows blockchain technology to prove what transactions actually have happened in the past, and game theory and economics incorporated in blockchain technology incentives stability and the blockchain platforms to survive in the long run (Wang K. , 2017). Buterin (Introduction to Cryptoeconomics, 2017) describes the key characteristics of Bitcoin in cryptoeconomics terms as two parts; firstly, the cryptography can be described as a toolset of:

- *Proof of work:* allows participants in the network to generate a proof that they have access to a certain amount of computation power. The result of a node performing a PoW task is a cryptographical proof that a certain amount of computational effort was performed.
- *Signatures*: A transaction can be signed with a signature. A signature provides a proof that the transaction sender is authentic.
- *Hashes*:
    - Hashes made it possible to validate the order of the transactions in the chain.
    - Hashes enable light client protocols via Merkle proofs; hence, hardware limited devices can also conduct transactions and generate proofs that these are valid.

Secondly, Bitcoin in cryptoeconomic terms can be described as a set of economic incentives:

- The miner of a block in the chain gets a specified amount of BTC, currently 12.5 BTC (blockexplorer.com, 2018), as reward for finding the block and additionally the miner "can extract rent from being temporary dictator over transaction inclusion" (Buterin, Introduction to Cryptoeconomics, 2017). Therefore, the miner of a block can temporary reject an actor from performing a transaction. The miner is incentivised to implement transactions with reasonable fees into blocks.
- The miner of a block that is not included in the chain gets no rewards.
- There is a difficulty adjustment, and the rewards are marginally zero sum in the long run. This suggests that all miners' total revenues will be roughly equal and only rely on their hashing power and this creates the selfish mining problem (Buterin, Introduction to Cryptoeconomics, 2017).

Furthermore, Buterin describes multiple types of economic incentives or disincentives that can be applied in blockchain platforms:

- *Rewards* incentives actors by increasing an actors balance or assigning them some privileges:
    - *Tokens or Coins* incentivize actors by awarding them a protocol-defined cryptocurrency, i.e. the block reward in Bitcoin. This protocol-defined cryptocurrency is scarce and therefore represents some value.
    - *Privileges* incentive actors by temporarily empowering them with decision-making rights, which can be used to extract rent. Other users of the network can 'bribe' an actor

that got the decision-making rights to include their transactions into a block, i.e. the transaction costs in bitcoin.

- *Penalties* disincentives actors to perform certain tasks, for example by reducing an actor's balance or remove them from future privileges.

Additionally, Buterin describes two concepts in cryptoeconomics that are somewhat similar.

- *Cryptoeconomic security margin:* defines a minimum amount of money loss X an actor has to spend for violating a protocol guarantee (Wang K. , 2017). "The basic idea is that it is possible to measure the security of a protocol in dollars" (Buterin, Introduction to Cryptoeconomics, 2017).
- *Cryptoeconomic proof*: A proof given by an actor in the format of a signed message, that states: "I certify that either P is true, or I suffer an economic loss of size X" (Buterin, Introduction to Cryptoeconomics, 2017).

Furthermore, Buterin argues that there are different economic assumptions for security models and different non-economic assumptions for security models. Some standard forms of non-economic assumptions for security models are:

- *Standardized byzantine fault tolerance*: This model assumes that 66.67 percentage of nodes in the network can be trusted.
- *Traditional fault tolerance:* This model assumes that all nodes in the network can be trusted, except some nodes that could crash.

Wang (Wang K. , 2017) and Buterin (Introduction to Cryptoeconomics, 2017) describe four cryptoeconomic assumptions of behaviour:

- *Honest majority model:* this model assumes that 51 % of the actors in a network function as trustworthy, i.e. the PoW mechanism uses this assumption.
- *Uncoordinated choice model:* This model assumes no coordination and alliances between nodes in a network and each node will have their own unique incentive. Furthermore, each node has a smaller capacity or stake than a predefined percentage of the network. This assumption represents the true "decentralization" idea behind the Bitcoin protocol.
- *Coordinated choice model:* This model assumes that a certain agent or organisation of agents controls each actor in the network. An example of this are the bitcoin mining pools where multiple actors mine under the command of the owner of a single mining pool.
- *Bribing attacker model:* This model starts with the assumptions made by the uncoordinated choice model, however adds the assumption that a malicious attacker is capable of making bribe payments to other actors conditionally of them taking a certain action. The bribing attacker model has two parameters:
    - *Budget*: How much is the attacker willing to pay for a conditional attack?
    - *Cost*: If the attacker does carry out the attack, how much is the attacker paying?

Above highlighted tools, models and assumptions describe the cryptoeconomical way of thinking and taxonomy that can be applied to understand blockchain platforms. Furthermore, cryptoeconomics can be used as a design toolkit for the design of a consensus mechanism. Blockchain enables users to enforce scarcity and facilitates value transfers. Through this viewpoint, cryptoeconomical systems change many fundamentals of how to incentivize human behaviour and therefore the potential of cryptoeconomical systems is massive (Evans, 2017).

3 Methodology

This chapter elaborates on the methodology chosen to answer the research questions. A qualitative design is selected, since this is most suitable to answer the 'how, why and what types of research questions defined in chapter 1.4. A quantitative design is not possible to research blockchain solutions since the technology is infancy. The research tries to describe blockchain technology from a holistic perspective, both describing the business as well as the technology perspective focusing on contemporary events. This research applies a multiple-case study method that is most appropriate to provide answers to the 'how and why' questions since there is no control over the events (Yin, 1984). The multiple-case study analyses three public blockchain technologies and focusses on the roadmaps delivered by the open source communities behind the blockchain technologies. Furthermore, information is used from developers' conferences and developers' community blogs. It is important to keep in mind that all developers have their own incentives and thoughts about problems and solutions, and therefore these findings are validated by in-depth semi-structured interviews with experts.

The main research question: *'How to qualify public permissionless blockchain technologies and why are these not wide-scale adopted for business use cases?'* is answered by combining the answers of the sub questions. The qualification of public blockchain technologies is conducted using the framework described by Saviotti and Metcalfe (1984) as a guideline in combination with a qualitative multiple-case study backed by a roadmaps analysis and in-depth interviews.

Sub question 1: *'How to characterise public permissionless blockchain technologies?'* is answered in the format of a conceptual model building upon the framework described by Saviotti and Metcalfe (1984).

Sub question 2: *'What are the essential design considerations in the selection of a public permissionless blockchain technology for business use cases?'* will be derived from the results of the multiple-case study and by several semi-structured interviews with multidisciplinary experts.

Sub question 3: *'What are the current challenges within public permissionless blockchain technology platforms and how will the blockchain communities solve these challenges?'* is answered by performing a multiple-case study. This case study is supported by the platform community roadmaps and attending and observing multiple expert conferences. Furthermore, the feasibility of the efforts to solve current challenges is validated by semi-structured interviews with experts.

This thesis can be divided in three parts, the literature review, the conceptual model and the multiple case study. The methodology regarding the thesis structure is described in the following subchapter.

3.1 Thesis structure

Conceptual model

The conceptual model used for this research builds upon the theory described by Saviotti & Metcalfe (1984), describing a blockchain technology as a set of service and technology characteristics. Figure 3.1, defines the scope of the model and provides an overview placing the conceptual model in the DLT space. As elaborated in the literature review blockchain is a kind of DLT. The focus of the research is on public permissionless blockchain technologies and the conceptual model can only be applied to this type.

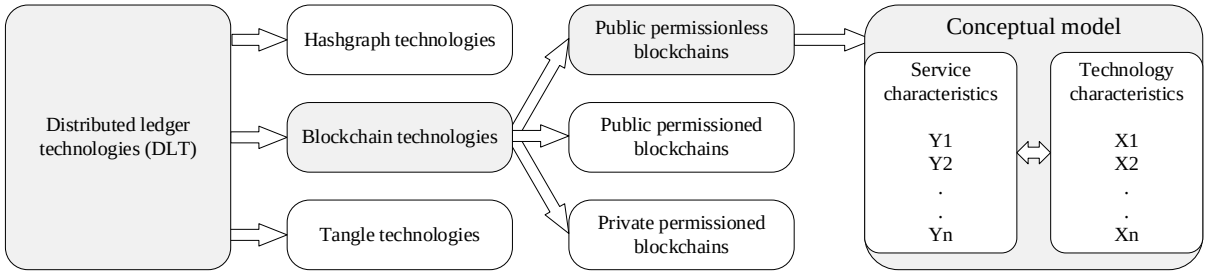


Figure 3.1 An overview of the conceptual model in the DLT space

Due to the fuzzy nature and infancy phase where blockchain technology is currently in, the conceptual model is drafted from the information acquired from unstructured interviews with experts, during expert conferences and from literature review. This collection information is structured in a conceptual model and this model is used as guideline for the case study.

Multiple case study

The multiple case study will be an in-depth qualitative research describing three different public permissionless blockchain technologies, i.e. Bitcoin, Ethereum and Cardano. The data for the case study is acquired from expert conferences, literature review and from developer community blogs. The conceptual model is used as research guideline to describe the characteristics of three public blockchain technologies. The case study will provide and in-depth overview of the three cases, describing the current challenges and solutions announced by the open source communities.

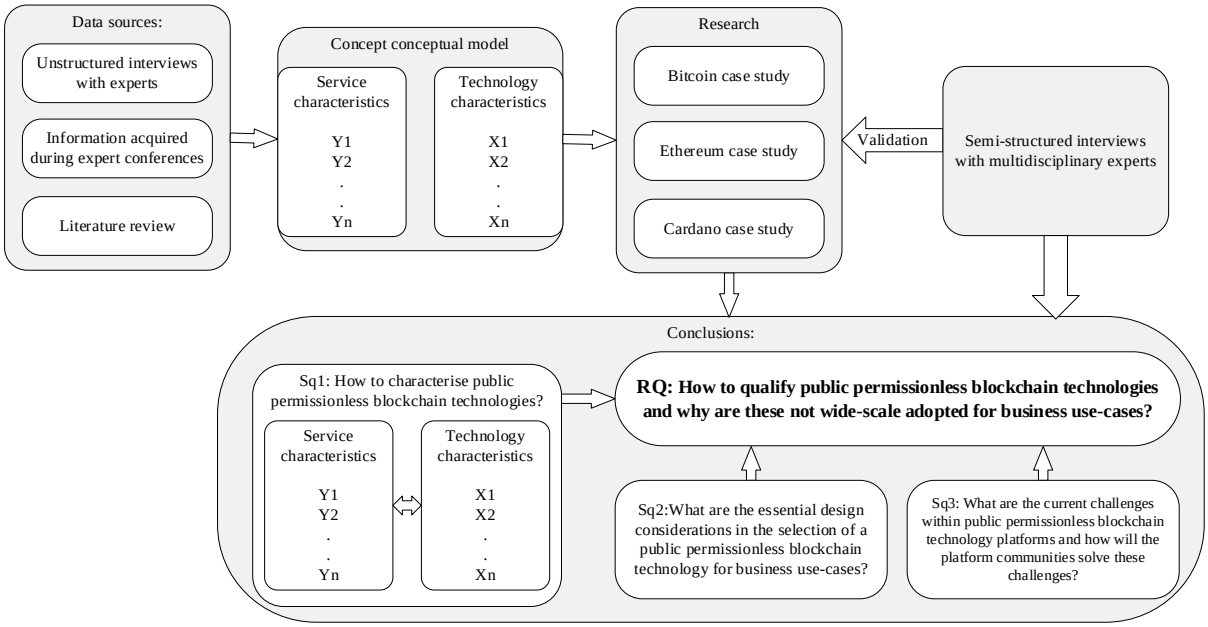


Figure 3.2 Research structure overview

3.2 Data collection

Due to the explorative and qualitative nature of this research, several face-to-face interviews are conducted in both unstructured and semi-structured ways. The unstructured interviews are conducted to create a broader understanding of blockchain technologies. The unstructured interviews are conducted during the conferences. Table 3.1 shows the list of attended conferences. The data acquired at the conferences and during the unstructured interviews is used complementary to the literature review for the creation of the conceptual model. Furthermore, insights are obtained from several meeting of the *Techruption Consortium Blockchain* (TCB) platform where experts from multiple parties are collaborating within a consortium to create a blockchain platform. These insights are used to validate the finding of this research. Since academic literature regarding blockchain technology is scarce, the case study uses data acquired at developers' conferences and developers' community blogs. The findings of the case study are validated by semi-structured interviews with multidisciplinary experts and during a presentation and open discussion at the blockchain innovation week for a large group of blockchain developers in The Hague. Table 3.2 shows the list of interviewees for the semi-structured interviews. Although the interviews are conducted in an open setting, two interview guides has been set up containing multidisciplinary questions. Appendix V shows the interview guides. All semi-structured interviews are recorded, transcribed and analysed using thematic analysis. The themes for the thematic analysis are distracted from the blockchain qualification framework introduced in chapter 4. The transcripts of the interviews are confidential and therefore not included in this report.

Table 3.1 List of attended conferences

Conference name:	place:	date:	Discussed topics:
UWV waarde wisselaar conference	Amsterdam	25-01-18	Deep dive into a pilot project called "Waarde wisselaar" for the Dutch government.
Dag van de Crypto	Amsterdam	29/30-01-18	Two days completely addressed to cryptocurrencies and *initial coin offerings* (ICOs)
Bitcoin Wednesday	Amsterdam	7-02-18	Smart Contracts, Drivechains, x86 VMs, Identity, Governance & Mass Surveillance
Blockchain Café, hosted by HU and Sogeti	Utrecht	15-02-18	Ethereum security and key management, Building a Dapp with non-fungible tokens, Ethereum in an enterprise context
Ethereum Community Conference ETHCC	Paris	8/9/10-03-18	Very broad Ethereum development conference focussed on identity, scalability privacy and governance.
Co-work day Blockchain030	Utrecht	19-03-18	Open co-work day with several blockchain developers and people with high blockchain interests.
Blockchain; hoe ziet dat eruit in de praktijk?	Utrecht	26-03-18	Blockchain as fact checker, HU blockchain lab, Blockrock podcast and DeepDive.training how to work with blockchain.
Tweakers.net Blockchain Meetup	Eindhoven	29-03-18	Blockchain beyond the cryptocurrency hype.
Bitcoin Wednesday	Amsterdam	02-05-18	Anonymity and Decentralization, Zcoin, SelfKey and Hashgraph
Co-work day Blockchain030	Utrecht	14-05-18	Open co-work day with several blockchain developers and people with high blockchain interests.
Blockchain innovation week	The Hague	25-05-18	In the week of the first pizza bought with bitcoin, we organize two full days on which experts share the newest developments and insights in blockchain technologies. The author of this thesis gave a talk about this research. Afterwards a discussion is held in order to validate the findings of this research.

Table 3.2 List of semi-structured interviewees

Interviewee name:	Company:	Date:
Bart Roorda	Blockchain Entrepreneur	14-05-18
Dan Acristinii	Head of R&D at Kryha	15-05-18
Oskar van Deventer	Senior scientist blockchain networking at TNO	03-05-18
Jarl Nieuwenhuijzen	Blockchain developer at Rabobank	29-05-18

4 Conceptual model

This chapter elaborates on the conceptual model derived from the literature review. The conceptual model has been set up using the Saviotti & Metcalfe (1984) ideology describing a product of service and technology characteristics that are interlinked by a pattern of mapping. Figure 4.1 shows the conceptual model describing the service and technology characteristics for public permissionless blockchain technology. The idea behind the conceptual model is to qualify blockchain services and technology very abstractly in order to create an all-encompassing framework that is usable as characterisation framework for public blockchain solutions. The framework is only applicable on public permissionless blockchain solutions, since other distributed ledger solutions and decentralized data storage solutions are out of scope and require a different set of technology characteristics. Each characteristic can be subdivided in multiple sub characteristics but for the sake of clarity, this chapter only elaborates on the basic characteristics. The characteristics within the framework can be only be used as guidance for the relative assessment of a public blockchain solution since blockchain technology is still in infancy and quantitative measurements are not possible. The following sections will describe the different concepts that are included in the conceptual model.

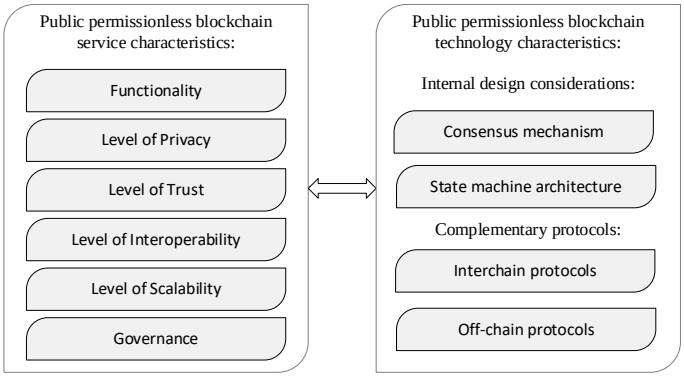


Figure 4.1 Basic conceptual model describing the six service characteristics and the four technology characteristics of blockchain technology

4.1 Identified service characteristics

Based on the literature review described in chapter 2, several unstructured interviews with experts and the attending of several expert conferences and meetups, this research introduces six service characteristics that qualify the services that a public blockchain technology could deliver in order to fulfil the requirements for blockchain use cases. Furthermore, the services provide a characterisation of public blockchain solutions. Each blockchain use case requires a different set of services in a public blockchain solution and these requirements are combined to a set of service characteristics.

4.1.1 Functionality

Oxford English Dictionary (2018) defines 'functionality' specifically for computer science as "the range of operations that can be run on a computer or other electronic system". The functionality characteristic of a public permissionless blockchain technology describes the set of functions that can be used by blockchain use cases. Each blockchain solution has a set of basic functionalities. For example, the main functionality of the Bitcoin blockchain is the cryptocurrency bitcoin.

4.1.2 Level of Privacy

Cambridge English Dictionary (2018) defines 'privacy' as "Someone's right to keep their personal matters and relationships secret". Privacy is a much-debated challenge of public blockchain solutions and different methods are researched to implement privacy into blockchain solutions. Additionally, privacy is a much-debated topic in Europe, since the new *General Data Protection Regulation* (GDPR) was adopted by the European parliament, the Council of the European Union and the European

Commission on the 14th of April 2016. The GDPR will be enforced on the 25th of May 2018 to strengthen and unify the data protection for all individuals within the European Union (Blackmer, 2016). The new GDPR regulation will replace the old 1995 EU Data Protection Directive. Two articles of the new GDPR regulations should be highlighted for blockchain use cases. Firstly, Art. 17 GDPR that describes the "Right to erasure ('right to be forgotten')" (Intersoft Consulting, 2018). This article brings challenges for public blockchain technologies since these have the characteristic of being immutable. Secondly, Art. 25 GDPR "Data protection by design and by default" that describes the data controller, i.e. the company holding the data, should implement technical and organisational measures such as pseudonymisation in order to meet the requirements of GDPR. This article creates both challenges and opportunities for blockchain solutions since blockchain technologies are immutable but also pseudonymous by default.

This research defines the 'level of privacy' characteristic as a service characteristic that public blockchain technologies can deliver for use cases. For example, a banks specific use case can require a blockchain technology that only stores pseudonymous information on-chain in order to comply with the new GDPR regulations.

4.1.3 Level of Trust

Cambridge English dictionary (2018) defines 'trust' as "the believe that someone is good and honest and will not harm you, or that something is safe and reliable". Therefore, in the case of a distributed ledger technology trust can be identified as believe that a ledger technology is good and honest and will not harm you and the technology is safe and reliable to use. Although trust is arguably a basic characteristic of public blockchain solutions, there are some exceptions where blockchains cannot be trusted completely. An example might be the case of a fork. In case a fork happens in a blockchain, it is unclear which fork is based on the truth and is trustworthy.

By introducing Bitcoin, Satoshi Nakamoto (2008) introduced an electronic payment system that relied on cryptographic proof without the need of a trusted third party. This leads to a paradigm shift from trusting third parties towards trusting cryptographic proofs. This research introduces the 'level of trust' characteristic as a service describing the security that a public blockchain solution can deliver for a specific use case.

4.1.4 Level of Interoperability

Cambridge Business English dictionary (2018) defines 'interoperability' as "the degree to which two products, programs, etc. can be used together, or the quality of being able to be used together". Therefore, in blockchain solutions interoperability is interpreted as the degree to which a blockchain is able to communicate to another blockchain with a certain quality without the need of an intermediary. This research introduces the 'level of interoperability' characteristic as a service enabling multiple public blockchain solutions to cooperate and exchange data and or value conjointly.

4.1.5 Level of Scalability

Cambridge English dictionary (2018) defines 'scalability' as "the ability of a business or system to grow larger". Therefore, in case of blockchain solutions, scalability can be described as the ability of a blockchain solution to grow larger. In the CryptoKitties use case, the Ethereum platform was not able to scale sufficiently with the growth of the CryptoKitties application resulting in a congested Ethereum platform. This research introduces the 'scalability' characteristic as a service enabling a blockchain solution to scale up in order to reach a use case's demand.

4.1.6 Governance

Cambridge English dictionary (2018) defines 'Governance' as "the way that organizations or countries are managed at the highest level and the system for doing this". Therefore, in case of blockchain solutions, Governance can be described as the way of managing the blockchain solutions at the highest

level. This research analyses public blockchain solutions, and therefore a decentralized governance process is required. This research introduces the 'governance' characteristic as a service enabling a blockchain solution to be governed in a decentralized mechanism.

4.2 Identified technology characteristics

Based on the literature review described in chapter 2, several unstructured interviews with experts and the attending of several expert conferences and meetups, this research introduces four technology characteristics that represent the technological building blocks of a public blockchain technology. According to Castaldi et al. (2009, p. 549), "technical characteristics represent the internal structure of the artefact and, in most cases, are the dimensions that the designers take into consideration". The four technology characteristics are interlinked with the service characteristics by a pattern of mapping. Due to complexity and the variegation of different public blockchain technologies, the four technology characteristics identified in this chapter are very broad and general to become all-encompassing and could discriminate in some sense. This research abstractly approaches the steps developers take during the design process of blockchain technologies. This process is qualified and divided into a set of technical characteristics.

Two out of the four concepts included in the set of technology characteristics are derived from a presentation of Adrian Brink who is the Core Developer & Head of Community of Tendermint and Cosmos. During the Ethereum developers' community conference in Paris from the 8th until the 10th of March 2018, Adrian Brink (2018) introduced a three-dimensional blockchain scaling approach that can be implemented with Tendermint. Tendermint is software that could securely and consistently replicating several applications in a distributed network. Tendermint combines a byzantine fault tolerance consensus mechanism with a Turing complete state machine (readthedocs.io, 2018). Tendermint decouples the state machine and the consensus mechanism to create a blockchain solution specifically built for specific use cases. The design approach of Tendermint is used to specify two technical characteristics, namely consensus mechanism and state machine architecture. Additionally, interchain protocols and off-chain protocols are included to qualify the technology characteristics of public blockchain technologies. This research introduces the consensus mechanism and the State machine architecture as internal design characteristics, since both describe the internal working of a blockchain. Additionally, this research introduces the Interchain and off-chain protocols as complementary protocols since they both are used as protocols able to expand the features or services of a blockchain solution working at a higher layer above blockchain technology. The upcoming subchapters elaborate provide an overview of the introduced technology characteristics.

4.2.1 Internal design considerations (IDCs)

Consensus mechanism

One important part of blockchain is the consensus mechanism. Chapter 2.2.4 provides an elaboration of consensus mechanisms. In public blockchain solutions, consensus mechanisms are currently much debated, since the consensus mechanism is a crucial part of blockchain solutions in order to reach mutual agreement about the state of the blockchain. Ethereum is currently planning to switch to a PoS based consensus mechanism called Casper. This research qualifies a consensus mechanism as an internal design consideration of a blockchain technology.

State machine architecture

According to Techopedia (2018), in science terminology the 'state' of an object describes the current physical makeup. In computer science, the 'state' of for example a computer program is similarly used and represent a computer program its current values or contents. According Buterin (Ethereum White Paper, 2014), from a technological point of view, bitcoin acts as a transaction-based 'state transition system'. The state in bitcoin consists of the ownership statuses of all bitcoin within the system. A transaction in the bitcoin blockchain thus leads to a change in the state. Wood (2014, p. 1) describes bitcoin as a "very specialised version of a cryptographically secure, transaction-based state machine".

Besides bitcoin, Ethereum can also be described as a state machine but with more functions and a more complex architecture. The state machine of Ethereum is called the *Ethereum virtual machine* (EVM), which is a Turing complete state machine. Turing complete means "that EVM code can encode any computation that can be conceivably carried out, including infinite loops" (Buterin, Ethereum White Paper, 2014). Besides Bitcoin and Ethereum, it is assumed that each blockchain has some implementation of a state machine to define its state. Therefore, this research qualifies a state machine architecture as an internal design consideration for a blockchain technology.

4.2.2 Complementary protocols (CPs)

Interchain protocols

The interchain concept is about combining multiple heterogeneous blockchain protocols and letting them interact in a cooperative manner (Brink, 2018; Burton, 2017). According Adrian Brink (2018), the world is moving towards a world of heterogeneous blockchains. This research qualifies 'Interchain protocols' as complementary protocols working on top of a blockchain technology expanding the features of a blockchain technology. An example of an interchain protocol is Interledger that is invented by Ripple enabling the connection of different heterogeneous blockchains (Interledger, 2018). An important note of this technology characteristic is that it is a complementary protocol that is considered blockchain agnostic enabling multiple heterogeneous blockchain to interconnect. An example of a use case in need of an interchain protocol is the decentralized exchange Barterdex. Barterdex has invented their own interchain protocol enabling atomic swaps of coins or tokens between heterogeneous blockchain platforms (Barterdex, 2018). In this case, Barterdex delivers an interoperability service within the ecosystem layer of a blockchain technology expanding the functionality of blockchain technologies.

Off-chain protocols

The off-chain protocol technology characteristic is, like the interchain protocol characteristic, an external blockchain characteristic. An off-chain transaction is the movement of value outside a blockchain in for example payments channels. An on-chain transaction is usually referred as a 'transaction' that represents the exchange of value on the chain between two accounts on the chain (Bitcoin Wiki, 2018). Multiple implementations of off-chain protocols are known in literature. Lightning networks for Bitcoin is an example of an off-chain protocol. This network enables bi-directional payment channels outside the bitcoin network. These payment channels can transfer bitcoin funds off the Bitcoin blockchain (Lightning Network, 2018). The main difference between the off-chain and interchain protocols is visualized in Figure 4.2. An off-chain protocol does not transact between two heterogeneous blockchain solutions, but creates a payment network off-chain, that can be settled after an amount of time on the blockchain.

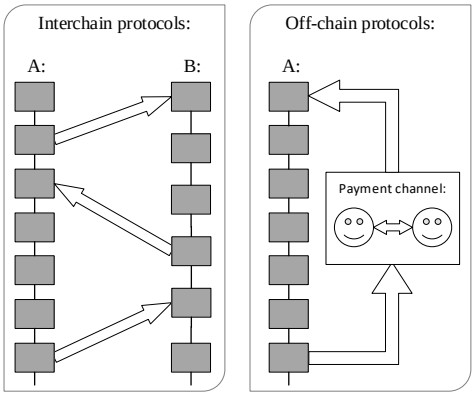


Figure 4.2 Comparison between interchain and off-chain protocols

5 Case study

This chapter elaborates on the empirical research describing three blockchain solutions in a case study format. The conceptual model described in Chapter 4 is used as guideline for this chapter. The case study will provide validation and further improvements to the conceptual model. The three cases elaborated in this chapter are Bitcoin, Ethereum and Cardano.

5.1 Bitcoin

Bitcoin is introduced in 2008 in a paper: "Bitcoin: A Peer-to-Peer Electronic Cash System" by someone, or a group under the pseudonym "Satoshi Nakamoto" and solved the double spending problem for electronic cash (Nakamoto, 2008). A common area of confusion talking about Bitcoin is the uppercase "B" versus the lower case "b". Bitcoin with a capital "B" is commonly associated to the payment network, and bitcoin with a lowercase "b" is commonly associated with the cryptocurrency BTC (Alyson, 2014). The software running the Bitcoin network is called Bitcoin Core. The latest version of Bitcoin core is 0.16.0 that was released on 26th of February 2018. The Bitcoin Core software, which is also known as the "Satoshi client", contains all aspects of the bitcoin system, including the wallets, a transaction verification engine and the copy of the entire blockchain and a full network node in the peer-to-peer Bitcoin network (Antonopoulos A. M., 2014). Bitcoin.org (2018) provides a version history of the latest Bitcoin Core versions including the changes made to the Bitcoin software. Bitcoin can be considered as an open source protocol since Bitcoin has no formal structure of governance. The standard way of communicating new ideas is by Bitcoin improvements Proposals (BIPs). A BIP is a design document that introduces new features or information to the Bitcoin community (Bitcoin Wiki, 2018).

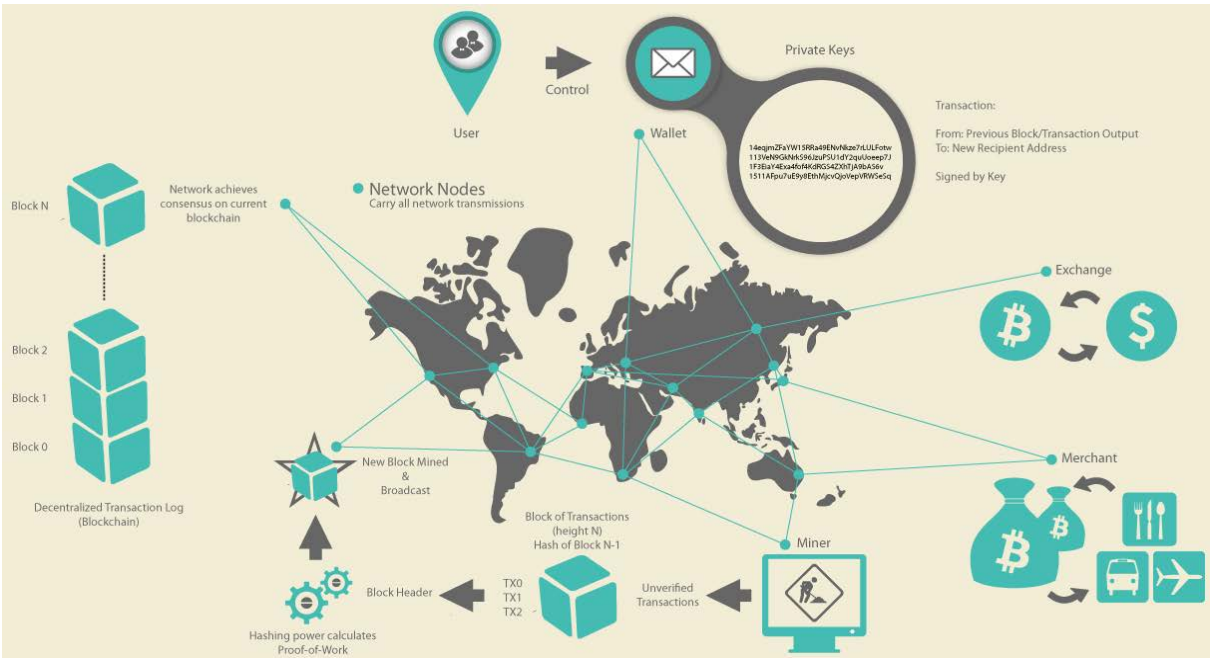


Figure 5.1 Bitcoin ecosystem overview. Adapted from Antonopoulos (2014)

Swan (2015) defines Bitcoin as the first generation blockchain denoted with version 1.0. She describes Bitcoin as cash and digital payment system for the internet, which can be considered as "Internet of money", without the requirement of a third party. Bitcoin already became the first global adopted decentralized transaction ledger (Wood, 2014). According to Morisse (2015), Bitcoin can be considered as a cryptocurrency ecosystem. Johansen (2017) defined ecosystems as "a coopetitive technology environment in which symbiotic relationships are formed to create mutual value for its members". Figure 5.1 shows the ecosystem of Bitcoin derived from Antonopoulos (2014). The bitcoin ecosystem exists of a group of users who control a single or multiple wallets, a group of full nodes storing and validating the blockchain and the miners that produce the blockchain by a consensus process.

Additionally, the ecosystem includes external parties that build complementary features on top of bitcoin, e.g. exchanges and merchants (Antonopoulos A. M., 2014).

This chapter introduces the service and technology characteristics of Bitcoin using the conceptual model introduced in chapter 4 of this thesis.

5.1.1 Technology characteristics

The blockchain technology that drives Bitcoin can be described as a set of technology characteristics. These technology characteristics include a set of IDCs and a set of CPs that are built on top or besides the Bitcoin blockchain to extend or improve the services. Table 5.1 provides an overview of the technology characteristics of Bitcoin derived from a variety of sources (Dinh, et al., 2017; Antonopoulos A. M., 2014; Sitepu, 2017). The upcoming subchapters provide a more in-depth overview of the different technology characteristics within Bitcoin.

Table 5.1 Bitcoin technology characteristics

	Technology characteristic:	**sub-characteristic:**	**Bitcoin implementation:**
IDC	*Network design*		Distributed (Peer-to-Peer)
	Consensus mechanism		PoW based on SHA-256
	State machine architecture	Coding language	Golang, C++
		Smart contract execution	Script
		Data structure	Transaction-based (UTXO)
		Block size	Measured in bytes: 1MB, ~2-4MB for a complete SegWit block.
		Block release time	targeted at ~ 600 seconds
		Block header data structure	Binary Merkle Tree with SegWit support since version 0.15.0
CP	*Complementary protocols*	interchain protocol	e.g. Decentralized exchanges, Interledger
		offchain protocol	e.g. Lightning (state-channel protocol)

Network design

Bitcoin works as a Peer-to-Peer network that operates as a networking layer on top of the Internet. The term Peer-to-Peer means that the computers that participate in the network are all peers to each other and each computer is equal in rights. The network of computers operates without a hierarchy in the format of a “mesh” network (Antonopoulos A. M., 2014). Therefore, the network design of Bitcoin can be characterised as a distributed network.

Consensus Mechanism

On top of the distributed network layer within Bitcoin runs the consensus mechanism of Bitcoin. The consensus mechanism used and introduced by Bitcoin is PoW. PoW is used to achieve consensus regarding the transactions that will be included in the blockchain. More specifically, miners have to proof their own integrity indirectly by providing a proof that they have performed a decent amount of work. An explanation of the PoW consensus mechanism is elaborated in chapter 2.2.4. The PoW scheme used in bitcoin is SHA-256 (Bitcoin Wiki, 2018). SHA stands for Secure Hash Algorithm, and SHA-256 is part of the SHA-2 cryptographic functions originally designed by the NSA. A much-debated point of discussion in the Bitcoin world is the ASIC. An Application-Specific Integrated Circuit (ASIC) is a specialized piece of hardware that only exists to perform a specific task (Smith, 1997). An ASIC is therefore much more efficient in performing the SHA-256 algorithm. Since the Bitcoin protocol automatically adjusts the mining difficulty to keep the block generation time around 600 second, the mining process with CPU’s or GPU has become economically unsustainable. Additionally, ASIC’s are often placed in large factory halls in mass amounts and several people argue that ASICs and the deployment of ASIC’s at industrial scale could lead to mining centralization (Calvin, 2017).

Furthermore, miners that do not possess an ASIC are discriminated since these users will not benefit from bitcoin mining efforts.

State machine architecture

The architecture running on top of the consensus mechanism is the state machine. Bitcoin can be considered as "a very specialized version of a cryptographically secure, transaction-based state machine" (Wood, 2014, p. 1). The state of Bitcoin represents a set of UTXOs stored in a decentralized transaction log. The decentralized transaction log is stored as "a chain of blocks" and each block contains a Merkle tree that secures all the UTXOs included in that block. Merkle trees are elaborated in chapter 2.2.3. If a new block, containing a new set of UTXOs is attached to the blockchain, the state of the blockchain changes towards a new state.

Transaction data structure

The decentralized transaction log contains a set of UTXOs. Each UTXO can be considered as a certain amount of unspent bitcoin corresponding to a bitcoin account. In bitcoin, if a transaction occurs, the transaction logics first verify the signatures of the sender. Then it verifies whether the amount of UTXO of the transaction output equals the amount of UTXO of the transaction input. Finally, if all steps are verified, the logic applies a change to the Bitcoin state and the transaction will be added to the unconfirmed transaction list. Bitcoin thus uses the amount of UTXO to track the account balances of users. The process of a single transaction is visualized in Figure 5.2.

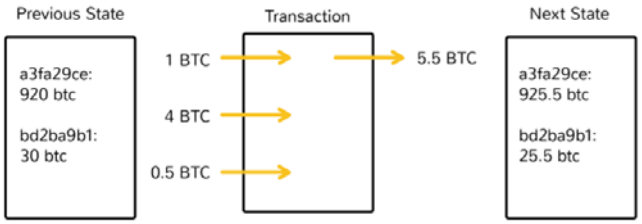


Figure 5.2 The process of a single transaction using the UTXO logic of Bitcoin. Adapted from Hertig & Kuznetsov (2018).

Smart contracts

According to Dinh et al (2017), all blockchains have built-in smart contracts that include their transaction logics. Additionally to this UTXO transaction logic, earlier versions of Bitcoin supported 200 opcodes that enable users to write scripts within bitcoin transactions, but many of those opcodes are disabled in some software updates for security reasons (Dinh, et al., 2017). These opcodes, or so-called Bitcoin "smart contracts", provide multi-signature features, bounty hunt contacts, time locks or a small 80 characters storage field (OP_Return). The name of this functionality within Bitcoin is "Script". These features are further elaborated in the service characteristics chapter of bitcoin.

Block size limits

A recent updated implemented in Bitcoin, but also in similar cryptocurrencies such as Litecoin, is *Segregated Witness* (SegWit). SegWit was activated in version 0.15.0 of Bitcoin Core at 14 September 2017. The soft fork implementing SegWit that was referred as BIP91 in the chain happened at block height 477120 at 21 July 2017 (Hertig, 2017; Bitcoin.org, 2018). A SegWit transaction is a normal transaction separated into two parts, the signature part ("witness data") and the transaction information holding the sender and receiver data. The maximum block size of bitcoin is currently 1MB and this limits the maximum amount of transactions that fit in a single block. In case of a SegWit transaction, only the transaction data is stored in the limited 1MB block Merkle tree, and the additional signature part will be stored in a newly added part of the Merkle tree that is not limited to the 1MB block limit. This SegWit block-design will effectively change the block size roughly ~2-4MB without changing the software that requires a hard fork (Bitcoin Wiki, 2018). Due to the larger effective block size, a complete SegWit block can store a higher amount of transactions in comparison to a non-SegWit block.

Additionally SegWit facilitates building other complementary protocols on top of Bitcoin such as the Lightning Network.

Complementary protocols

Bitcoin is not in the possession of a built-in method to exchange information with other heterogeneous blockchains, e.g. let a user exchange some funds between two blockchains. However, due to the "smart contract" features and SegWit implementation within Bitcoin transactions several complementary protocols are possible to exist on top of Bitcoin to extend the service characteristics. One currently much debated project is the Lighting network. This protocol is elaborated in chapter 5.1.4. Another example of a complementary protocol is a decentralized exchange. Due to the opcodes enabling multi-signature and time lock features within Bitcoin, several decentralized exchanges have been created. These decentralized exchanges perform atomic swaps (komodoplatform.com, 2018). Atomic swaps allow users to trade crypto within users their own wallet. The in-depth workflow of a decentralized exchange is outside the scope of this research. Another form of a complementary protocol currently designed by Ripple is called the "Interledger protocol". The Interledger protocol works on top of bitcoin and other distributed ledger technologies and has as purpose to increase the interoperability characteristics of blockchains and DLTs (interledger.org, 2018).

5.1.2 Service characteristics

The services delivered by Bitcoin can be described as a set of service characteristics. Table 5.2 provides an overview of the service characteristics of Bitcoin. The upcoming subchapters provide a more in-depth overview of the different service characteristics of Bitcoin.

Table 5.2 Bitcoin service characteristics

Service characteristic:	**sub-characteristic:**	**current level:**
Functionality	Native functionalities	Cryptocurrency BTC, limited Turing incomplete "smart contracts" and SegWit
	Add-on functionalities	Lightning Decentralized exchanges
Level of Privacy	User level privacy	Pseudonymous
	Transaction level confidentiality	Open and accessible
Level of Trust	Security	High
	Finality	No absolute finality
	Liveness	High
Level of Interoperability		(currently) Poor
Level of scalability	Maximum throughput	3.3 – 7 TX/sec
	Latency	~10 minutes *
	Transaction costs	Pay per byte: >1 USD per transaction at 12-4-18
Governance	Incentives	Depends per stakeholder type
	Mechanism for Coordination	Off-chain by Bitcoin Improvement Proposals (BIPs) and developers mailing list. On-chain by miners who have the power to implement protocol changes.

Functionality

The service characteristic functionality can be divided in native functions and add-on functions. A native function of Bitcoin is the *bitcoin cryptocurrency* (BTC). Additionally, Bitcoin provides a set of add-on functionalities.

bitcoin cryptocurrency (BTC)

Nakamoto (2008, p. 1), introduced Bitcoin as "a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution". Therefore, the main functionality of Bitcoin is the bitcoin cryptocurrency. The bitcoin blockchain enables everyone without restrictions to send and receive bitcoin. Spenkelink (2014) defines cryptocurrency as "a digital medium of exchange that relies on a decentralized network that facilitates a peer-to-peer exchange of transactions secured by public key cryptography". Besides this definition, Huls (2015) highlighted four characteristics of cryptocurrencies, which are Peer-to-Peer, code similarity, unregulated and cryptography. The characteristics can be interpreted for bitcoin as following:

- *Peer-to-Peer*: bitcoin is a peer-to-peer cryptocurrency. It does not require a central party to exchange bitcoin between two users of the network. There is no central authority involved, and therefore no persons can be excluded from the network. Additionally there is no single point of failure, and therefore a centralized DDOS attack will not affect the network.
- *Code similarity*: "Bitcoin is a technology, but it expresses money which is fundamentally a language for exchanging value between people" (Antonopoulos A. M., 2014, p. 4). Bitcoin could become a standard for exchanging value over the internet. Additionally the code of bitcoin is open source, updated and improved by the community. If the community cannot reach an overall agreement, a fork could happen leading to two different blockchain solutions, e.g. Bitcoin Core and Bitcoin Cash.
- *Unregulated*: bitcoin is a borderless medium of exchange that is not backed by a government or central bank. Governments around the world are trying to govern Bitcoin, but they are not able the govern BTC itself (Martindale, 2017). Therefore, the price of the coins is volatile and based on scarcity, supply and demand. The amount of issued BTC is controlled by the protocol. The coins are "mined" by the PoW executers of the network, and each block comes with a new amount of UTXO rewarded to the miner. The amount is regulated by the protocol, started with 50 BTC per block in 2009 that is reduced roughly every four years in half. Currently, the block reward is set at 12.5 BTC but will be reduced towards 6.25 BTC at block 630000 with an estimated time to be mined around May 2020. The maximum amount of BTC ever is set at 21 million, and will be achieved probably around 2140 (Bitcoin Wiki, 2018).
- *Cryptography*: Each transaction within the Bitcoin network is secured by cryptography, and trust is ensured within the distributed network where users do not directly trust each other (Sitepu, 2017). Each actor in the network hold one or multiple private keys as addresses of identification and stores their private key on a secure place. The combination of the private and public key enables a user to conduct a transaction. If a transaction had happened it is considered to become immutable, i.e. the transaction cannot be reversed in the future.

The bitcoin cryptocurrency is the main feature of the Bitcoin blockchain technology. Additionally, the bitcoin cryptocurrency itself has a set of use cases: Firstly, the bitcoin cryptocurrency is used as incentive mechanism to maintain the integrity of the bitcoin blockchain. Secondly, the cryptocurrency is used to pay for transaction cost, and thirdly, the cryptocurrency is used as a digital medium of exchange. Chapter 2.2.5 treats cryptoeconomics that include both the economic incentive mechanism and cryptography solutions combined to explain blockchains.

Add-on functionalities

Bitcoin supports a limited format of smart contracts functions that can be merged together with a bitcoin transaction. The "smart contract" functions in bitcoin are called "opcodes" that introduce additional features to bitcoin transactions. The functions include:

- *Multi-signature* enables a wallet to require multiple signatures to authorize a transaction. A normal transaction within bitcoin is called a "single-signature" transaction, which only requires one signature. Multi-signature enables multiple applications, e.g. husband and wife petty cash

joint account, Two-factor authentication wallets, decentralized cold storage vault (Bitcoin Wiki, 2018).

- *Timelock* adds the feature to restrict spending a certain amount of bitcoin until a specified future time or block height. This feature in bitcoin enables multiple applications, e.g. payment channels, hashed Timelock contracts and decentralized exchanges (Bitcoin Wiki, 2018).
- *Data-output (OP_return)* adds an extra field to a transaction where users can add custom messages. An interesting aspect of this data field is that the first ever bitcoin transaction placed in the genesis block includes the text: "Chancellor on brink of second bailout for banks", that was a title of the main article in the New York Times of the 3th of January 2009. The text was probably intended as proof that that block was created on or after the 3th of January 2009. This text is still accessible in the considered immutable Bitcoin genesis block. This field can thus be used to assign intellectual property in a hash format. The hash of the data is stored in the blockchain, and the owner of a hashed document can proof that he or she was in possession of the document at a certain time, without releasing the document (Bitcoin Wiki, 2018).

The latter functions and SegWit are used to build applications on top of Bitcoin to expend its features, such as Lightning and decentralized exchange services. These services can potentially influence the other service characteristics described that are elaborated below. Lightning could potentially increase the level of privacy, scalability and interoperability characteristics of Bitcoin. The OP_return field is in practice much used for timestamping. If a hash from another blockchain or document is stored on the Bitcoin blockchain, the data corresponding to that hash can be considered immutable since the hash is stored forever. This enables other blockchain platforms to store their transaction history on bitcoin in a hash format, ensuring their immutability.

Level of Privacy

Bitcoin currently does not possess internal account privacy or confidential transaction protocols. This means that each transaction on Bitcoin can be traced back until the block where the unspent bitcoin is awarded to the miner. Additionally the balance of each public key on the ledger is open and accessible. The public key on the ledger is pseudonymous by design, although the boundary between bitcoin and fiat currency is regulated. If a user wants to buy bitcoin or another cryptocurrency with fiat currency, i.e. Euro or Dollar, regulators have obligated exchanges to ask for legal identification. This allows governments to link the pseudonymous accounts to legal identifications and since the transactions histories of each bitcoin account are openly accessible, governments are able to track the bitcoin spending and receiving of an account. There are some proposals to increase the level of privacy within bitcoin. The bitcoin wallet from bitcoin core is a deterministic wallet. This type of wallet generates multiple public addresses from a single master key (Bitcoin Wiki, 2018). This enables some level of privacy on the user side, since a deterministic wallet enables a bitcoin user to have many different public keys in a single wallet and a user does not reuse its addresses. The user can swap coins between these public keys. Furthermore, complementary protocols such as lightning and or decentralized exchanges can potentially increase the confidentiality of transactions. Lightning for example enables peer-to-peer payment channels, and only the sum of all payments between two parties within the channels will be stored within the blockchain when a channel is closed. The decentralized exchange Barterdex will implement a Zcash layer, which potentially enables confidential atomic swaps (Barterdex, 2018). Both methods will increase the level of privacy by increasing transaction confidentiality on bitcoin; however, each privacy mechanism above does not truly enables private bitcoin transactions or addresses. The pseudonymous account balances stored on-chain are still open and accessible.

Level of Trust

Although the Level of Trust is hard to measure, this research interprets the level of trust in Bitcoin as follows; the security of the Bitcoin network, the liveness of the Bitcoin network and the finality of a Bitcoin transaction.

Security of Bitcoin Network

The security of Bitcoin is very high, since the network itself is never hacked. The hacks described by many newspapers describe only hacks of centralized exchanges or private keys of users. If a user stores its private keys securely, the bitcoin of that particular user can be considered secure. Additionally, Bitcoin has the most secure PoW consensus mechanism since the hashing power of the network is the highest among other blockchain networks. The current estimated hash rate of used for the Bitcoin PoW mechanism is 39.180.231 tera hashes per second (Blockchain.info, 2018). This extremely high hash rate uses much energy, however makes it extremely difficult to perform a successful 51% attack on Bitcoin.

Liveness of the Bitcoin network

There are multiple descriptions of liveness within blockchain solutions. The liveness of a blockchain can relate to the consensus mechanism. For the consensus mechanism, the liveness of PoW is considered high, since the blockchain will not stop if a single node fails operating. Eventually the longest chain will be dominant. Additionally the liveness can also be considered as the uptime of the Bitcoin network. Due to its distributed nature, the uptime is considered very well although several attack vectors related to Liveness of the Bitcoin network can be found in literature (Bitcoin Wiki, 2018). The first attack is a Dust attack, sending large amount of low value transactions to congest the network. This type of attack leads to higher transactions cost. The second type is a DDOS attack, although this type of attack is considered unfeasible due to the distributed nature of the Bitcoin network. An attacker has to DDOS all network nodes at once.

Finality of bitcoin transaction

The finality of a bitcoin transaction is always probabilistic due to the nature of its consensus mechanism PoW. However, in practice, many parties assess a transaction to be finite after six blocks confirmations (Buterin, On Settlement Finality, 2016). Therefore, a transaction is considered final in practice in one hour after the confirmation.

Overall, the trust in Bitcoin can be considered relatively high, although it takes some time for a transaction to become finite. Therefore, applications that require immediate transaction finality could have problems using bitcoin as payment method.

Level of Interoperability

The native level of Interoperability of Bitcoin is considered poor, since the protocol itself does not support direct communication with other blockchains. Complementary solutions such as Lightning, Interledger and decentralized exchanges are currently creating methods of interoperability with other heterogeneous blockchain solutions (Barterdex, 2018; Lightning Network, 2018).

Level of Scalability

The definition of scalability within blockchains is often discussed in literature since the increasing popularity of public blockchains clarifies the scalability issues of current public blockchain implementations. Croman et al. (2016) introduces four key metrics to analyse the scalability of blockchain solutions. The metrics are Maximum throughput, Latency, Bootstrap time and Cost per Confirmed Transaction (CPCT). Maximum throughput stands for the maximum rate at which a blockchain can confirm transactions. Latency is the time it takes for a transaction to confirm. Bootstrap time describes the time for a new node to download and process the complete blockchain and get up to speed with the rest of the network and CPCT is the cost in USD for the complete system to confirm a single transaction. The following paragraphs describe the level of scalability of Bitcoin. Additionally the growth in size of a blockchain can be considered as a scalability issue since each full node has to store the complete blockchain. Bootstrap time and blockchain size growth are not included in this report since it is not relevant for blockchain use cases.

Maximum throughput

The maximum throughput of bitcoin is related to the maximum effective block size, the targeted block time, and the average transaction size in a block (Croman, et al., 2016). The maximum throughput assuming a 1MB block size and a block time targeted at 600sec is between 3.3 and 7 transactions per second depending on the transaction size. The SegWit update potentially doubles this maximum throughput because the effective block size is doubled. The lightning network enables a higher throughput, a lower latency, and a lower CPCT; however, it still takes a transaction to sign off an amount of funds on-chain to open a lightning payment channel between two parties (Lightning Network, 2018).

Latency

The Latency definition is slightly discriminating with the transaction finality definition described in in chapter 2.2.3. Croman et al. (2016) argue that they define latency as the time to obtain a single confirmation. Some payment processors accept zero-confirmation transactions while other require a decent amount of finality and wait six block confirmations before accepting a payment. This depends on the amount of certainty of payment required for a use case. The time to obtain a single confirmation in Bitcoin is roughly 10 minutes and is related to the block time of 10 minutes. This rule only applies for an uncongested network where the transactions come with a decent amount of fee, which incentivise miners to include the transaction in a block.

Cost per Confirmed Transaction (CPCT)

According to Croman et al. (2016), CPCT encompasses several distinct resources to keep the Bitcoin network running and secure. The CPCT can be explained as operation cost (mainly electricity) and capital equipment costs including:

- *Mining costs:* The expending's of miners to complete the PoW puzzle and generate a new block
- *Transaction validation costs:* The cost that is spend to perform the required computation for the validation of a transaction.
- *Bandwidth costs:* The cost of network resources to keep the network in sync including all transactions, the blocks and the metadata.
- *Storage costs:* The cost of storing the complete blockchain, which is required for each full node and each miner.

It is very hard to measure these metrics, since energy prices, amount of transactions per second, hardware prices and many other variables continuously fluctuate. Croman et al. (2016) argues that based on their calculations the cost per confirmed transaction is between $1,40 and $2,90 in which 57% of the price is for mining electricity. Although these prices are debatable, the transactions cost should be at least equal to the transactions cost to create a sustainable business model in the future if block rewards drop. This makes Bitcoin transactions currently quite expensive due to high transaction cost. According to bitinfocharts.com (2018), the current transaction price (12-04-18) is below 1 dollar, although the average transaction price at the 22th and 23th of December 2017 was even higher than 50 dollar. This high transaction cost was the result of a congested Bitcoin network. In case of a congested network, the users are willing to pay a higher transaction fee in order to push their transaction into the network. Since the focus of this research is on use cases, the average transaction costs will be important for the consideration of a blockchain solution for a specific use case.

Governance

Multiple perspectives of analysing governance and blockchain are possible, since the governance of blockchain is often poorly understood, and often treated in different contexts (Ehrsam, 2017). One important characteristic of a public blockchain is that it is borderless and distributed. A consequence of this characteristic is that governments cannot directly regulate blockchains. This research describes governance as a service characteristic that could be implemented within the design of a public

blockchain solution and by the community supporting the blockchain. Ehrsam (2017) describes two critical components of governance that are incentives and mechanism for coordination.

Incentives

Ehrsam (2017) describes three groups of stakeholders, which uses the incentive mechanisms that are incorporated within Bitcoin. These stakeholders are Bitcoin core developers, Bitcoin miners and Bitcoin users. Each stakeholder group has its own incentives to put effort in Bitcoin. The incentives for each stakeholder group are as following:

- *Bitcoin core developers* are incentivized by the potential future value increase of token holdings, the benefit from social recognition and the potential future power to stay in control over the network.
- *Bitcoin miners:* are incentivized by the potential future value increase of token holdings, by expected future block rewards and the released transaction fees coming with the generation of a future block.
- *Bitcoin users* are incentivized by the potential value increase of token holdings, speculation, or the increase in potential features and services e.g. time-stamped documents.

Above incentives should be balanced and positive for each the stakeholder group in order to create a sustainable network (Ehrsam, 2017). Another effect that incentivizes the users of using the blockchain is the so-called network effects. If more stakeholders start using and mining within the network, the higher the level of trust in the network will become. This potentially increases the network value.

Mechanism for coordination

Mechanism for coordination can be subdivided in two parts, on-chain and off-chain coordination mechanism. Two off-chain coordination mechanism within bitcoin are the BIPs and the Bitcoin developers' mailing list. These two-coordination mechanisms are set in place in order to reach consensus between developers about potential future updates. The first BIP (BIP 0001) was set up by Amar Taaki on 19th august 2011 and explains what a BIP is (BIP GitHub, 2018). According to Bitcoinwiki (2018) three types of BIPs exist:

- *Standard Track BIPs* entail the potential on-chain changes of the Bitcoin network protocol, the blocks, transaction validation methods or anything related to interoperability. This type of BIP requires community consensus to be applied.
- *Informational BIPs* entail several design issues or general guidelines. This type of BIP does not propose any new Bitcoin features, is about providing information and does not require community consensus.
- *Process BIPs* describe a new process or a change within an existing process. Overall, this BIP is comparable with the Standard Track BIPs; however, the proposed changes are off-chain.

BIP and the mailing list are examples of off-chain coordination mechanism that are set up for and by developers to reach consensus about future updates of Bitcoin. If the Developers reach consensus about a potential update, Miners have to signal for an amount of blocks wheter they agree with the new version of the protocol or not. Within bitcoin, this method is called signalling. If more than 95% of the miners agree on the update, the update will be implemented in the new version of Bitcoin (Lombrozo, 2017). Therefore, finally the miners are responsible for the on-chain protocol changes since they have the power to generate new blocks and accept or reject a potential protocol change.

5.1.3 Bitcoin characterisation framework

Table 5.3 shows the characterisation model of Bitcoin derived from the case study. The model describes the service characteristics and the technology characteristics of the Bitcoin technology. Currently, Bitcoin has several challenges. Each challenge mentioned relates to a service characteristic. The

challenges can potentially be solved by improving or changing a single or a set of technology characteristics. It should be noted that each use case does not have equal requirements, i.e. not each use case does require the level of interoperability characteristic. The first challenge is related to functionality. Functionality in bitcoin is limited and bitcoin does not seems intentional to become a smart contract platform, however second layer solutions such as RSK enable smart contract functionality (RSK, 2018). The second challenge is related the level of privacy. Bitcoin does not have native privacy protocols and the complete bitcoin blockchain is open and accessible to everyone. The third challenge is related to level of trust. Although bitcoin is the most secure due to the extremely high hash rate, there is no absolute finality. The fourth challenge is related to the level of interoperability. Bitcoin does not possess native functionality to exchange information with other ledgers. The fifth challenge is regarding the level of scalability. Currently the throughput of bitcoin is between 3.3 and 7 transactions per second. Additionally, the average digital cost per transaction for a bank is ~$0,17 (Shevlin, 2014) and is around ~$1,00 for Bitcoin (Bitinfocharts, 2018). In addition, future transaction prices are not predictable due to cryptocurrency price fluctuations and other influencing factors. The sixth challenge is regarding the Governance of Bitcoin. Due to the conservative slowly changing nature of the Bitcoin community, potential upgrades for the software are introduced very slowly. However, this characteristic also ensures a higher level of trust. Most of the challenges above mentioned are trade-offs for the current implementation of Bitcoin to ensure the highest possible level of trust. Although the list is short, the upcoming chapter shortly elaborates on the potential future upgrades for bitcoin.

Table 5.3 Bitcoin described as a set of service and technology characteristics

Services characteristics		
current level	*sub-characteristic*	*main characteristic*
Cryptocurrency BTC, limited Turing incomplete "smart contracts" and SegWit	Native functionalities	**Functionality**
Lightning decentralized exchanges	Add-on functionalities	
Pseudonymous	User level privacy	**Level of Privacy**
Open and accessible	Transaction level confidentiality	
High	Security	**Level of Trust**
No absolute finality	Finality	
High	Liveness	
(currently) Poor		**Level of Interoperability**
3.3 – 7 TX/sec	Maximum throughput	**Level of scalability**
*~10 minutes **	Latency	
>1 USD (12-4-18)	Transaction costs	
Depends per stakeholder	Incentives	**Governance**
Off-chain by Bitcoin Improvement Proposals (BIPs) and developers mailing list. On-chain by miners who have the power to implement protocol changes.	Mechanism for Coordination	

Technology characteristics		
main characteristic	*sub-characteristic*	*implementation*
Network design		*Distributed (Peer-to-Peer)*
Consensus mechanism		*PoW based on SHA-256*
State machine architecture	Coding language	*Golang, C++*
	Smart contract execution	*Script*
	Data structure	*Transaction-based (UTXO)*
	Block size	*Measured in bytes: 1MB, ~1.8MB for a complete SegWit block.*
	Block release time	*Targeted at ~ 600 seconds*
	Block header data structure	*Binary Merkle Tree with SegWit support since version 0.15.0*
Complementary protocols	interchain protocol	*Decentralized exchanges*
	offchain protocol	*Lightning (state-channel protocol)*

5.1.4 Roadmap

The last months SegWit is implemented within Bitcoin, and the lightning network is available in beta phase on the main network. Lightning promises to bring a network of micropayment channels that potentially can solve the scalability issue within Bitcoin (Poon & Dryja, 2016). Lightning is a decentralized off-chain network that uses Bitcoin's opcodes and SegWit implementations. Within lightning, transactions can be transmitted over a network of micropayment channels, in other words payment channels, and the transfer of these funds does virtually occurs off-chain. Two users open a bidirectional payment channel by signing off a spending of funds (Lightning Network, 2018). If the channel is open, the two users can exchange funds off-chain without broadcasting them to the blockchain. By creating a network of two parties' payment channels, it is possible to exchange funds over the lightning network with all parties connected to the network. The participants of this so-called Lightning network are able to transact bitcoin over the Lightning network at high volume and high speed without congesting the Bitcoin network. When a user finishes, the user always has the opportunity to close the channel, settlement will take place and the user exits the lightning network. The minimal viable product (MVP) of lightning only interacts with one blockchain. Future versions of Lightning networks will connect multiple heterogeneous blockchains enabling cross-chain atomic swaps within the lightning network (Lightning Network, 2018). Currently, the lightning network is available in beta phase on the Bitcoin network. The micropayments channels fall under the more general state-channels protocols. A state-channel enables blockchains to become more efficient by moving many processes off-chain.

Besides lightning networks, there are other speculations about multiple new implementations for bitcoin in the upcoming years such as MAST, Schnorr signatures, Bullet-proofs, Confidential transactions, Sidechains and Mimblewimble (Edwards, 2018), however it is still unclear which of those updates will reach implementation phase. The bitcoin community can be characterized as very conservative and hesitant in order to stay the most trustworthy cryptocurrency. Currently, the only Bitcoin community driven future planning is described by the BIP list, however this list is highly technical and almost not understandable for the non-technical users.

5.2 Ethereum

Towards the end of 2013, Vitalik Buterin who was a young programmer and Bitcoin enthusiast, started working on a project to expand the features of Bitcoin. He mentioned that multiple projects, such as Bitcoin, Namecoin, Peercoin and Mastercoin were limited in features and were mainly focused on fulfilling one particular feature. His vision was to build a universal blockchain solution, able to fulfil multiple features. For his project, he recognized that building a project directly on top of Bitcoin would lead to struggles with initial constraints of Bitcoin; hence, he started developing a complete new system from scratch. In December 2013, Vitalik Buterin came up with a "white paper" that outlined the initial idea behind Ethereum; "A next generation smart contract & decentralized application platform" (Buterin, Ethereum White Paper, 2014). Ethereum was introduced as "a blockchain with a build-in Turing complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own rules of ownership, transaction formats and state functions" (Buterin, Ethereum White Paper, 2014). Shortly after the release of the whitepaper, Gavin Wood reached out to Vitalik and they both started working on the protocol layer of Ethereum. According to Antonopoulos & Wood (2018), the founders of Ethereum just like Satoshi Nakamoto, did not invented a new technology, but they combined new and old inventions together. Arguably, this form of innovation can be considered as a form of recombinative innovation in order to create a new radical innovation.

Ethereum is often described as "the World Computer"; however, this definition is quite vague. Antonopoulos & Wood (2018) describe Ethereum both from a computer science and from a practical perspective. "From a computer science perspective, Ethereum is a deterministic but practically unbounded state machine with two basic functions; the first being a globally accessible singleton state, and the second being a virtual machine that applies changes to that state. From a more practical perspective, Ethereum is an open source, globally decentralized computing infrastructure that executes programs called smart contracts. It uses a blockchain to synchronize and store the system state along with a cryptocurrency called ether to meter and constrain execution resource cost." (Antonopoulos & Wood, 2018). Ethereum can be considered as a decentralized blockchain app platform that runs application exactly as programmed without any downtime, censorship or fraud. The apps running on the blockchain platform are executed by the EVM and have direct access to built-in economic functions that require the Ether cryptocurrency. The main purpose of the Ether cryptocurrency is not to function as a digital currency payment network like bitcoin, however Ether is intended as a utility cryptocurrency to pay for the use of the Ethereum platform. Each computation on the platform requires an amount of gas. The gas price is often expressed as Gwei, and currently one ether is equal to 10^9 Gwei.

The development process of Ethereum is defined in four development stages codenamed Frontier, Homestead, Metropolis and Serenity (Gupta, 2015). The Metropolis stage is divided in two hard forks implementations codenamed Byzantium and Constantinople. Currently Ethereum is at the Metropolis Byzantium stage. Antonopoulos & Wood (2018) provided an overview of the past hard forks within Ethereum that can be linked to the development stages. These hard forks are visualized together with corresponding development stages in Table 5.4.

Table 5.4 Ethereum phases of development. Adapted from (Antonopoulos & Wood, 2018; Karnjanaprakorn, 2017).

Development stage / Hard fork codenames	Block number of transition	Description
Frontier	0	The Frontier phase was the first live release of the Ethereum Main network, allowing developers to experiment, mine ether and start building Dapps and tools for the Ethereum platform. The Frontier phase of Ethereum lasted from July 2015 until March 2016
Frontier – Ice Age	200.000	A hard fork that introduced an exponential difficulty increase for PoW, and in the long run claimed to motivate a transition towards PoS.
Homestead	1.150.000	The second stage of Ethereum, was considered the first production release, and brought many protocol improvements that laid the foundation for future upgrades. The Homestead phase of Ethereum lasted from March 2016 until October 2017.
Homestead – DAO fork	1.192.000	This hard fork reversed the hacked DAO contract, and caused a split of the community leading to Ethereum and Ethereum Classic.
Homestead – Tangerine Whistle	2.463.000	This hard fork fixed a bug in the Gas calculation that could be exploited by a denial of state attack.
Homestead – Spurious dragon	2.675.000	A hard fork addressing denial of service attack vectors, and a state clearing.
Metropolis – Byzantium	4.370.000	Metropolis Byzantium is the first Hard fork of the Metropolis phase, which was launched in October 2017. This hard fork introduced multiple updates such as permitted zkSNARKs features (Ethereum Team, 2017).
Metropolis - Constantinople	Future planned	This hard fork is expected to include the switch to the first version of Casper FFG that implements a hybrid PoW/PoS model. Additionally Metropolis provides some tooling for non-technical users to create a more user friendly Ethereum. The last phase of the Metropolis update is expected for mid-2018.
Serenity	Future planned	Serenity is the fourth and final stage of Ethereum. This phase was initially planned for early 2018 but this is already delayed. The goal of this phase is to implement the complete Casper update going to a PoS consensus mechanism.

Ethereum can be considered as an open source protocol since Ethereum has no formal structure of governance. Identical to Bitcoin, the standard way of communicating new ideas is by *Ethereum improvement Proposals* (EIPs). An EIP is a design document that introduces new features or information to Ethereum.

According to Swan (2015), Ethereum can be denoted as a second-generation blockchain; however, this label is not perfect. The projects classified by Swan as blockchain 2.0 are smart contracts, smart property, distributed applications (Dapps), Distributed Autonomous Organisations (DAOs) and Decentralized Autonomous Corporations (DACs). Although these types of projects can be built upon Ethereum, Ethereum is a more generalized platform continuously changing to enable novel and unaddressed use cases. Therefore, the label blockchain 2.0 for Ethereum seems to be too specific and will probably become incorrect in the future. According to Wood (2014, p. 1), "Ethereum is a project which attempts to build the generalized technology; technology on which all transaction-based state machine concepts may be built". In comparison to bitcoin, which is classified as a cryptocurrency ecosystem, The Ethereum platform enables the foundation for other ecosystems on top of it. However, research still shows that ecosystems' building on top of blockchain platform is still in its early stages (Johansen, 2017).

This chapter threats the service and technology characteristics of Bitcoin using the conceptual model introduced in chapter 4 of this thesis.

5.2.1 Technology characteristics

The blockchain technology that drives the Ethereum platform can be described as a set of technology characteristics. These technology characteristics include a set of IDCs and a set of CPs that are built on top or besides the Ethereum blockchain to extend or improve the services. Table 5.5 provides an overview of the technology characteristics of Ethereum derived from a variety of sources. The upcoming subchapters provide a more in-depth overview of the different technology characteristics within Ethereum.

Table 5.5 Ethereum technology characteristics

	Technology characteristic:	sub-characteristic:	Ethereum implementation:
IDC	*Network design*		Distributed (Peer-to-Peer)
	Consensus mechanism		Ethash, which is a PoW memory-hard considered ASIC resistance consensus mechanism, based on SHA-3 Keccak-256.
	State machine architecture	Coding language	Solidity, Serpent, LLL, Vyper, Bamboo
		Smart contract execution	EVM
		Data structure	State (Account-based), Transactions and Receipts
		Block size measured in Gas	~8000000 Gas (19-4-18)
		Block release time	Target is ~ 12 seconds
		Block header data structure	Merkle Patricia Trees, and uncle blocks
CP	*Complementary protocols*	interchain protocol	e.g. Decentralized exchanges, Interledger
		offchain protocol	e.g. Raiden Network

Network Design

Communication between the Ethereum nodes and clients is arranged by the DEVp2p wire protocol. The Ethereum network can be reached on TCP port 30303 (Ethereum Wiki, 2015). Ethereum can be considered as a Peer-to-Peer network, since all nodes can connect to each other and are equal. The DEVp2p protocol enables a mesh network, and therefore the network design of Ethereum can be characterised as a distributed network (Github.com, 2018). Table 2.2 shows an overview of a distributed network design.

Consensus Mechanism

On top of the distributed network layer within Ethereum runs the consensus mechanism of Ethereum. The consensus mechanism of Ethereum can be characterised as an internal design consideration to reach consensus about the state of the chain. The consensus mechanism currently used by Ethereum is a PoW based mechanism called Ethash. PoW is used to achieve consensus regarding the transactions that will be implemented in the blockchain. A more elaborated explanation of the PoW consensus mechanism can be found in chapter 2.2.4. The PoW scheme used in Ethereum is Keccak-256 (Ethereum Wiki, 2017). Ethash is considered memory intensive, and this limits the benefit of ASIC mining over traditional GPU mining. According to the Ethereum Wiki (2015), Ethash is intended to satisfy the following goals:

- *IO saturation*: The mining process should consume the entire memory bandwidth of the processing unit; this is a strategy towards ASIC resistance.
- *GPU friendliness*: The developers tried to make mining by GPU's as easy as possible. This create a higher incentive for GPU card users to conduct in the mining process, leading to larger and better distributed mining network.
- *Light client verifiability*: A light client should be able to verify one round of mining in under 0.01 seconds, in order to create a blockchain that can be validated by light clients. The goal is that each device should be able to verify the network, enabling small and lightweight IOT devices to access the network.
- *Light client slowdown*: If a user is a light client, the process of verifying a block should be much slower than an identical process on a full client. This is another strategy towards ASIC resistance.
- *Light client fast start-up*: A light client should become operational and able to verify new blocks within 40 seconds using JavaScript.

The latter design goals have already solved the ASIC problem that is currently of influence for Bitcoin PoW. However, the PoW mechanism of both Ethereum and Bitcoin are still energy consuming. The

Ethereum foundation is currently working on Casper FFG, which is a hybrid PoW/PoS consensus mechanism. Since Casper FFG is currently not implemented on the Ethereum Main network and is on the roadmap for mid-2018, Casper FFG is further elaborated in chapter 5.2.4.

State machine architecture

The architecture running on top of the consensus mechanism is the state machine. “Ethereum, taken as a whole, can be viewed as a transaction-based state machine: we begin with a genesis state and incrementally execute transactions to morph it into some final state” (Wood, 2014, p. 2). Within bitcoin, each block header contains one Merkle tree storing all UTXO transactions within a block. Ethereum stores three different Merkle trees per block that all three store different kind of objects, which are Transactions, Receipts (Pieces of data showing the effects of each transaction) and the State (Buterin, Merkling in Ethereum, 2016). The Merkle trees used within Ethereum are Patricia Merkle Trees. This means that the Merkle trees between the block are also interlinked to change for example account states. Figure 5.3 shows an overview of the Merkle Patricia tree structure between two blocks within the Ethereum blockchain.

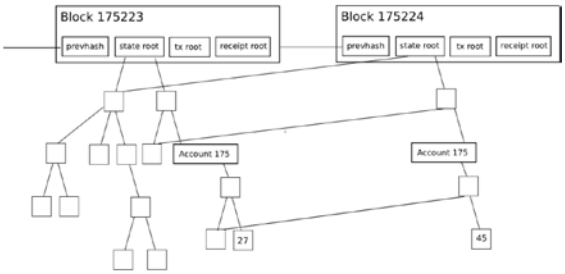


Figure 5.3 Merkle Patricia tree of the state-root within Ethereum. Adapted from Buterin (2016)

The block time-release time in Ethereum is on targeted by the protocol at ~12 seconds. Because this time relatively short, it is hard for all mining nodes to stay in sync with the network. Sometimes it happens that a nodes thinks that a block is not implemented in the chain yet and that node is mining block N, however another mining node (e.g. on the other side of the world) is already one block ahead, which is block N+1. This creates the risk of blocks becoming a “stale”, i.e. not being part in the main-chain. In order to provide an incentive for the of-sync node for its mining, the block is still added to the chain as uncle block and this uncle block receives a part of the block reward (Buterin, Uncle Rate and Transaction Fee Analysis, 2016).

Transaction data structure

Bitcoin uses the UTXO transaction model to address balances to a bitcoin account. Ethereum uses an account-based transaction model. Figure 5.4 shows an overview of how a transaction works according to the account-based transaction model within Ethereum.

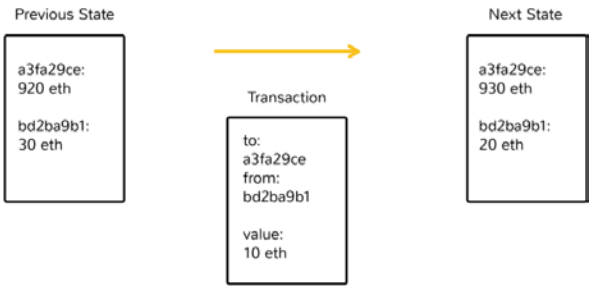


Figure 5.4 The process of a single transaction using the account-based transaction model. Adapted from Hertig & Kuznetsov (2018)

Smart contracts

In relation to Bitcoin, Ethereum provides a much more extensive smart contract language. Bitcoin currently only support some amount of opcodes to put some logic to a transaction. Ethereum however has implemented its own virtual machine, the EVM, to run Ethereum bytecode. The coding languages that come that can be compiled into the bytecode are Solidity, Serpent, LLL, Vyper and Bamboo (Dinh, et al., 2017). “The EVM is a quasi-Turing complete machine; the quasi qualification comes from the fact that the computation is intrinsically bounded through a parameter, gas, which limits the total amount of computation done” (Wood, 2014, p. 19).

Block size limits

Bitcoin has a maximum block size to address the maximum amount of bytes a block can store. In Ethereum, a block has a Gas limit. The amount of Gas is related to the processing capacity of a block. This keeps the maximum processing time to validate a block low and keep the blockchain accessible for low power devices. The gas size of a transaction describes the amount of computation required. Currently the gas limit is ~8000000 gas (19-4-2018).

Complementary protocols

Ethereum is not in the possession of a built-in method to exchange information with other heterogeneous blockchains, e.g. let a user exchange some funds between two blockchains (atomic swaps). However, due to the “smart contract” features several complementary protocols are feasible to exist on top of Ethereum to extend the service characteristics. Identically to Bitcoin, decentralized exchanges and the Interledger protocol both support Ethereum plug-ins (Castillo, 2017). As alternative for the Lightning network, Ethereum has Raiden Network. Raiden Network is identical in functionality to Lightning Network and is designed as complementary protocol for Ethereum to solve scalability issues. A minimal viable product of Raiden Network, µRaiden is already available on the Ethereum main network since September 2017. µRaiden enables payments or state-channels between two parties to exchange Ethers or ERC20 tokens. Whereas Raiden Network allows multiparty payments over a network of bidirectional payment channels (Karapetsas, 2018).

5.2.2 Service characteristics

The services delivered by the Ethereum platform can be described as a set of service characteristics. Table 5.6 provides an overview of the service characteristics of Ethereum. The upcoming subchapters provide a more in-depth overview of the different service characteristics of Ethereum.

Table 5.6 Ethereum service characteristics

Service characteristic:	sub-characteristic:	Current level:
Functionality	Native functionalities	Ether cryptocurrency, quasi-Turing complete EVM to run smart contracts
	Add-on functionalities	Endless applications possible relying on (non)-fungible tokens and identity contracts.
Level of Privacy	User level privacy	Pseudonymous
	Transaction level confidentiality	Standard open and accessible, obfuscated transactions possible with zkSNARKs.
Level of Trust	Security	High
	Finality	No absolute finality
	Liveness	High
Level of Interoperability		Poor native capability
Level of scalability	Maximum throughput	31.66 TX/sec for ether transactions
	Latency	~12 seconds
	Transaction costs	Pay for Gas in Gwei: Simple Ether transaction: ~0,30 USD at 24-4-18.
Governance	Incentives	Depends per stakeholder type
	Mechanism for Coordination	Off-chain by Ethereum Improvement Proposals (EIPs) and Ethereum Request for Comments (ERC) standards. On-chain by gas limit voting.

Functionality

The service characteristic functionality can be divided in native functions and add-on functions. A native function of Ethereum is the *Ether cryptocurrency* (ETH). Additionally, Ethereum provides a set of add-on functionalities that uses the EVM to add logic to the chain. Ethereum describes itself as a platform where ecosystems can built upon.

Ether cryptocurrency (ETH)

The Ether cryptocurrency has almost equal characteristics as the bitcoin cryptocurrency. However, there is a large difference in the usage of the currency for the Ethereum platform itself. Ether is the native cryptocurrency for the operation of Ethereum. Ether is used to pay for gas that can be classified a unit to pay for transaction fees and computational services of the EVM (Wood, 2014). This EVM is a decentralized Turing complete virtual machine that can execute Turing complete smart contracts. Therefore, the EVM capable of running smart contracts is directly related to the Add-on functionalities of the Ethereum platform.

Add-on functionality

According to Buterin (Ethereum White Paper, 2014), there are multiple types of applications that can run on top of Ethereum and are programmable in smart contracts. Firstly, it is possible to generate a token system on Ethereum. Secondly, identity and reputation systems can built upon the Ethereum platform. Additionally DAOs and applications like saving wallets, crop insurance, decentralized data feeds, smart-signature escrow, Cloud computing, Peer-to-peer gambling, prediction markets and on-chain decentralized marketplaces are possible. Overall, since the EVM is quasi-Turing complete, the possibilities in terms of functionality within Ethereum are endless and possible not all use cases are currently known. This sub-chapter briefly explains some of the functionalities within Ethereum.

Tokens

Ethereum knows several standards for programming token contracts on the Ethereum platform. The most used token contract is defined as ERC20 and is proposed by Fabian Vogelsteller on the 19th of

November 2015. The ERC20 standards define a set of common rules that an Ethereum token has to implement. The ERC20 standard provides the ability for developers to build their own token contract on the Ethereum platform. The ERC20 token became a popular standard for crowdfunding companies that are starting their own ICOs. The most prominent example of an ERC20 tokens is EOS. At the time of writing EOS has a market cap of 9,42 billion USD that is completely backed by an ERC20 token that runs on the Ethereum platform. The ERC20 tokens are characterised as fungible tokens. According to Genestroux (2018), A fungible tokens has two main characteristics.

- *Only the quantity matters*: If two users possess the same fungible tokens, these tokens are indistinguishable. If both users have the same amount of tokens, the tokens represent the same value and the users can exchange them.
- *Any amount of it can be "merged"*: Each amount of tokens can be merged together to create a large amount of the tokens.

A non-fungible token is distinguishable and each token can have its own characteristics. The tokens cannot be merged together and scarce tokens could represent a higher value. The first well-known application example for non-fungible tokens is CryptoKitties (0xcert, 2018). CryptoKitties enables the breeding and trading of virtual cats on Ethereum. Each cat is represented by a non-fungible token and has unique properties. A CryptoKitty is a collectible on the Ethereum platform, and this is one of the first applications using non-fungible token contracts (Collet, 2018). Other applications for non-fungible tokens are identities.

Identity and reputation systems

Additionally to the ERC20 token contract, Fabian Vogelsteller has recently proposed the ERC725 Ethereum identity standard (Braendgaard, 2018). This standard enables the management of user identities on Ethereum. The ERC725 is a proposal for an Ethereum identity solution, however additionally to this solution there are other identity solutions built upon Ethereum such as uPort. The ERC725/ERC735 Identity standard enables identity claims between parties on Ethereum. Party A could for example claim on an ERC725/735 contract on Ethereum that party B has a passed the KYC process of Party A. Party B can proof to Party C on-chain that Party A has checked KYC for Party B. Although, above solutions are limited, the first implementations of identities on Ethereum are currently discovered.

Overall, the functionality of Ethereum is endless and the first "killer" applications running on the Ethereum platform are currently being released, i.e. CryptoKitties.

Level of Privacy

In contradiction to Bitcoin, Ethereum already has implemented an internal privacy protocol. This protocol enables confidential transactions on the Ethereum blockchain. Before the implementation of this protocol, Ethereum had similar privacy characteristics as Bitcoin. This means that each transaction on the Ethereum blockchain can be traced back until the block where the Ether is awarded to the miner. In addition, each public key or address within Ethereum is pseudonymous, and regulators regulate the exchanges where fiat currencies can be exchanged to Ethers. Similar to bitcoin, decentralized exchanges and state-channel protocols enable private add-on functionalities to Ethereum.

During Devcon3, which is the main developers' conference of the Ethereum community, Ethereum latest software upgrade, Metropolis - Byzantium was announced. This upgrade includes the zkSNARKs technology that enabled confidential transactions on Ethereum. According to Reitwiessner (2016), zkSNARKs are highly mathematical and hard to understand but very important for Ethereum. The possibilities of zkSNARKs are very impressive, and the technology made it possible to check the correctness of computations without knowing wat was executed, and perform this efficiently. Simplistically, zkSNARKs enables confidential transactions between two accounts on Ethereum (Lundkvist, 2017).

Level of Trust

Although the Level of Trust is hard to measure, this research interprets the level of trust on the Ethereum platform as follows; the security of the Ethereum network, the liveness of the Ethereum network and the finality of transaction on Ethereum.

Security of Ethereum network

The security of Ethereum is very high, since the network itself is never hacked. The hacks described by many newspapers describe only hacks of centralized exchanges or private keys of users such as the parity hack. During this hack, an unexperienced user accidentally locked 300 million USD worth of Ether from multiple users in a multi signature wallet. This was not a security issue of the Ethereum network; however, an issue in the Multi signature wallet built on Ethereum from Parity (Akentiev, 2017). Another hack was the DAO hack in 2016 that is already treated in chapter 1.2.2. This hack was related to an issue within the smart contract of the DAO. The real problem of security is thus not related to the Ethereum network itself, but to the developers that write the smart contracts. Therefore, smart contracts are susceptible for human errors. The Ethereum community currently propose ERC standards for smart contracts to reduce the chance of human error for developers. Since Ethereum runs on the PoW consensus mechanism, another security measure for the Ethereum network is the total amount of computation power that miners put into the Ethereum network. The Ethereum Network Hash Rate is currently 276 TH/s according to etherscan.com (Etherscan, 2018). Arguably, the hash rate is very high, and a 51% mining attack can be considered unfeasible. Additionally, no 51% attacks of the Ethereum main network can be found in literature. In comparison to Bitcoin, the hash rate of Ethereum is very low; however, this can be explained by the ASIC resistance Ethereum Ethash PoW consensus mechanism.

Liveness of Ethereum network

There are multiple descriptions of liveness within blockchain solutions. The liveness of a blockchain can relate to the consensus mechanism. For the consensus mechanism, the liveness of PoW is considered high, since the blockchain will not stop if a single node fails operating. Eventually the longest chain will be dominant. Within Ethereum, the longest chain is calculated as the total sum of the block difficulties. The chain with the highest difficulty is dominant (Ethereum StackExchange, 2017). Additionally the liveness can also be considered as the uptime of the Ethereum network. Due to its distributed nature, the uptime of the EVM is considered very high.

Finality of a transaction on Ethereum

The finality of an Ethereum transaction is always probabilistic due to the nature of its consensus mechanism PoW. However, in practice, many parties assess a transaction to be finite after six blocks confirmations (Buterin, On Settlement Finality, 2016). Therefore, a transaction is considered final in practice in roughly 72 seconds after the confirmation, since the targeted block time on Ethereum is 12 seconds.

Overall, the Level of Trust characteristic of Ethereum can be considered very high. The biggest issue lies within the centralized smart contracts programmed by developers. Since every developer is able to build applications upon the Ethereum platform, the apps are prone to human error where a malicious user can take an advantage off. An example of a bug in a smart contract was the DAO. The problem of the DAO is described in chapter 1.2.2.

Level of Interoperability

Similar to Bitcoin, the level of Interoperability of the Ethereum platform is considered poor since the protocol itself does not support direct communication with other blockchains. Complementary solutions such as Raiden networks, decentralized exchanges and Interledger will probably create methods of interoperability with other heterogeneous blockchain solutions; however, these solutions did not proof themselves yet.

Level of Scalability

Similar to Bitcoin, the level of scalability is an important challenge within the Ethereum platform. The application CryptoKitties created a congestion crisis on Ethereum. The Dapp CryptoKitties app grew significantly and required a significant amount of CryptoKitties transactions. This leaded to a congested Ethereum platform, resulting in ICO delaying their release date, and users waiting days for their transactions to be included (ConsenSys, 2018). Equally, to bitcoin, this chapter treats the maximum throughput, the latency and the CPCT of the Ethereum platform as level of scalability metrics.

Maximum throughput

The maximum throughput of Ethereum is related to the Gas limit of a block, the targeted block time and the average gas per transaction in an Ethereum block. Additionally, since the main purpose of the Ethereum platform is not to perform Ether transactions specifically, it is very hard to qualify the maximum throughput in terms of transactions. However, the maximum throughput for simple ether transaction is easy to calculate. A simple transaction cost 21000 gas and the current gas limit per block is ~8000000 gas (ethstats.net, 2018). This leads to a maximum of ~380 transactions per block, and with the targeted block time of 12 seconds, a maximum throughput of ~31.66 transactions per seconds is possible. This amount of transactions per second only applies for simple Ether transactions.

Latency

The Latency definition is slightly discriminating with the transaction finality definition described in chapter 2.2.3. Croman et al. (2016) argue that they define latency as the time to obtain a single confirmation. Some payment processors accept zero-confirmation transactions while other require a decent amount of finality and wait six block confirmations before accepting a payment. This depends on the amount of certainty of payment required for a use case. The time to obtain a single confirmation within Ethereum is roughly 12 seconds and is related to the targeted block time of 12 seconds. This rule only applies for an uncongested network where the transactions come with a decent amount of fee, which incentivise miners to include the transaction in a block. During the CryptoKitties congestion, the mempool grew significantly and transaction latency went up to days for several users that did not want to pay a higher amount of gas for their transaction.

Cost per Confirmed Transaction (CPCT)

According to Croman et al. (2016), CPCT encompasses several distinct resources to keep the Bitcoin network running and secure. The CPCT of Ethereum will be slightly different and can be explained as operation cost, which is mainly electricity, and capital equipment costs including:

- *Mining costs:* The expending's of miners to complete the PoW puzzle and generate a new block
- *Computation validation (gas) costs:* The cost that is spend to perform the required computation for the validation of a transaction.
- *Bandwidth costs:* The cost of network resources to keep the network in sync including all transactions, the blocks and the metadata.
- *Storage costs:* The cost of storing the complete blockchain, which is required for each full node and each miner.

It is very hard to measure these metrics, since energy prices, amount of transactions per second, hardware prices and many other variables continuously fluctuate. The cost per confirmed transaction of Ethereum cannot be found in literature, but is considered lower that bitcoin's CPCT, since the Ethereum network is more efficient in terms of transactions per second. Additionally, Ethereum is not specifically made for Ether transactions, and therefore, the cost per confirmed computation would be a better metric for Ethereum. According to bitinfocharts.com (2018), the current price (24-04-18) for a simple transaction on Ethereum is around ~0.30 dollar, although the average transaction price at the 10th of January 2018 was even higher than 4 dollar. This high transaction cost was the result of a congested Ethereum network due to the massive pump and dump token sale of January. In the case of a congested

network, the users are willing to pay a higher transaction fee in order to push their transaction into the network. Since the focus of this research is on use cases, the average transaction costs will be important for the consideration of a blockchain solution for a specific use case. As reaction to the congested network problems, Vlad Zamfir who is a researcher at the Ethereum Foundation and the lead developer at the Casper protocol upgrade posted a message on twitter that Ethereum is "still not safe or scalable" (Zamfir, VladZamfir, 2018).

Governance

The governance characteristic of Ethereum is currently slightly similar to Bitcoin. (Ehrsam, 2017). This can potentially change if Ethereum implements Casper, although some articles contradict this (Zamfir, Against on-chain governance, 2017). The upcoming subchapters elaborate on the governance characteristic of Ethereum and the differences between Bitcoin and Ethereum.

Incentives

The incentives model of Ethereum is similar to bitcoin. Ehrsam (2017) describes three groups of stakeholders, which uses the incentive mechanisms that are incorporated within Ethereum. These stakeholders are Ethereum developers, Ethereum miners and Ethereum users. Each stakeholder group has its own incentives to put effort in Ethereum. The incentives for each stakeholder are as follows:

- *Ethereum developers* are incentivized by the potential future value increase of token holdings, the benefit from social recognition and the potential future power to stay in control over the network.
- *Ethereum miners:* are incentivized by the potential future value increase of token holdings, by expected future block rewards and the released transaction fees coming with the generation of a future block.
- *Ethereum users* are incentivized by the potential value increase of token holdings, or the increase in potential features and smart contracts capabilities.

Above incentives should be balanced and positive for each stakeholder group in order to create a sustainable network. Current weaknesses in the model are the low incentives for developers, and the over reliance in Ethereum creator Vitalik Buterin (Ehrsam, 2017), although some articles contradict this as well (Zamfir, Against on-chain governance, 2017).

Mechanism for coordination

Within the Ethereum community, there is some unclarity about the taxonomy of the mechanisms of coordination. Vlad Zamfir (Against on-chain governance, 2017) has argued that the taxonomy regarding Ethereum its governance is not properly documented. Additionally, he claims that Ethereum currently only applies off-chain governance mechanisms. He defines on-chain governance as "the idea that the blockchain nodes automatically upgrade when an on-chain governance process decides on an upgrade and that it is time to install it" without the requirement of a hard fork (Zamfir, Against on-chain governance, 2017). This chapter tries to summarize the governance mechanism of coordination within Ethereum. The mechanism for coordination can be subdivided in two parts, on-chain and off-chain coordination mechanism. Two off-chain coordination mechanism within Ethereum are *the Ethereum Improvement proposals* (EIPs) and the *Ethereum Request for Comments* (ERCs). According to Antonopoulos & Wood (2018), "An EIP is a design document providing information to the Ethereum community, or describing a new feature for Ethereum or its processes or environment. The EIP should provide a concise technical specification of the feature and the design rationale. The EIP author is responsible for building consensus within the community and documenting dissenting opinions". An EIP can have four statuses (Ethereum Community, 2018):

- *Draft:* An EIP that is open for consideration
- *Accepted:* An EIP that is planned for immediate adoption in the next hard fork.

- *Final:* An EIP that is already accepted and adopted in a previous hard fork.
- *Deferred:* An EIP that is rejected and needs some improvements.

An ERC is an Ethereum version of a Request for Comments (RFC). An ERC is a publication from someone in the Ethereum community, which describes an application level technical standard, i.e. for writing a smart contract. These two-coordination mechanisms are set in place as off-chain governance processes for potential future upgrades or smart contract standards. Additionally, Ethereum allows miners to adjust the maximum block size dynamically by voting on the gas limit. This can be considered as a form of on-chain mechanism for coordinating the network capacity of Ethereum.

5.2.3 Ethereum characterisation framework

Table 5.7 shows the characterisation model of Ethereum derived from the case study. The model describes the service characteristics and technology characteristics of the Ethereum technology. Currently, Ethereum has several challenges. Each challenge mentioned relates to a service characteristic. The challenges can potentially be solved by improving or changing a single or a set of technology characteristics. It should be noted that each use case does not have equal requirements, i.e. not each use case does require an equal set of service characteristics. The first challenge is regarding the Level of Privacy characteristic. Current accounts on Ethereum are only pseudonymous and obfuscation on account level is currently impossible. Additionally, transactions on Ethereum are open and accessible unless the zkSNARKs protocol is used; however, these transactions are very large and therefore very expensive to perform on Ethereum. The second challenge is related to the level of trust. Although the level of trust is high overall for Ethereum and proven by the past, there is no absolute finality currently possible by Ethereum. Additionally, developers' program smart contracts that run on Ethereum and this is prone to human error. The Ethereum community currently supplies ERC standards for smart contracts to reduce the chance of human error for developers. The third challenge is regarding the level of interoperability. The Ethereum platform does currently not possess native functionality to exchange information with other ledgers. The fourth challenge is regarding the level of scalability. Scalability of blockchains is a very much-debated topic. Currently the maximum throughput of Ethereum is 31.66 TX/sec for simple transactions and this is extremely low in comparison to centralized ledger based solutions such as VISA. Additionally, transaction costs are roughly equal to a bank transaction at $ 0.30. In addition, transaction costs are very volatile and not predictable due to cryptocurrency price fluctuations and other influencing factors. Furthermore, the size of the Ethereum blockchain has exceeded 1TB, and this rapid growth is not sustainable (Schoedon, 2018). The fourth challenge is regarding the Governance of the Ethereum platform. Currently, the mechanism for coordination seems slightly centralized and several articles have claimed that Vitalik Buterin, Ethereum founder, has too much control. Additionally voting for potential upgrades is slow and partly centralized to the Ethereum Foundation. Although above challenges are serious of concern, there are potential projects solving above challenges for Ethereum. These projects are elaborated in the upcoming chapter.

Table 5.7 Ethereum described as a set of service and technology characteristics

Services characteristics		
Current level	*sub-characteristic*	*main-characteristic*
Ether cryptocurrency, quasi-Turing complete EVM to run smart contracts	Native functionalities	**Functionality**
Endless applications possible relying on (non)-fungible tokens and identity contracts.	Add-on functionalities	
Pseudonymous	User level privacy	**Level of Privacy**
Standard open and accessible, obfuscated transactions possible with zkSNARKs.	Transaction level confidentiality	
High	Security	**Level of Trust**
No absolute finality	Finality	
High	Liveness	
Poor native capability		**Level of Interoperability**
*31.66 TX/sec**	Maximum throughput	**Level of scalability**
*~12 seconds **	Latency	
Pay for Gas in Gwei: Simple Ether transaction: ~0,30 USD at 24-4-18.	Transaction costs	
Depends per stakeholder type.	Incentives	**Governance**
Off-chain by Ethereum Improvement Proposals (EIPs) and Ethereum Request for Comments (ERC) standards. On-chain by gas limit voting.	Mechanism for Coordination	

Technology characteristics		
main-characteristic	*sub-characteristic*	*implementation*
Network design		*Distributed (Peer-to-Peer)*
Consensus mechanism		*Ethash, which is a PoW memory-hard considered ASIC resistance consensus mechanism. Based on SHA-3 Keccak-256.*
State machine architecture	Coding language	*Solidity, Serpent, LLL, Vyper, Bamboo*
	Smart contract execution	*EVM*
	Data structure	*State (Account-based), Transactions and Receipts*
	Block size	*~8000000 Gas (19-4-18)*
	Block release time	*Targeted at~ 12 seconds*
	Block header data structure	*Merkle Patricia Trees, and uncle blocks*
Complementary protocols	interchain protocol	*e.g. Decentralized exchanges, Interledger*
	offchain protocol	*e.g. Raiden Network*

5.2.4 Roadmap

Although there is no official Ethereum Roadmap, there are three mayor projects currently on the planning besides the Raiden Network implementation. As observed at the ETHCC, which is probably the largest Ethereum development community conference of Europe, the community is currently putting much effort in these three projects. The projects are trying to solve the current scalability challenges within Ethereum as a combined effort. The upcoming sub-chapters briefly describe the current projects led by the Ethereum community to solve the current challenges within the Ethereum blockchain space.

Casper

Rosic (2017), wrote a relative easy to read guide of the current Ethereum Casper implementation. Currently the Ethereum blockchain uses a PoW mechanism to reach consensus over the blockchain. The biggest concerns of PoW are that it is a very energy consuming and slow mechanism of reaching

consensus. To solve this issue, the community is currently working on the transition towards a PoS based consensus mechanism called "Casper". The first implementation of Casper is already working on an alpha test network since the 1st of January 2018 (Murray, 2018), and the main network implementation of Casper FFG is currently planned for the Metropolis Constantinople hard fork upgrade, which is currently scheduled for mid-2018. The general PoW and PoS consensus mechanism are treated in chapter 2.2.4.

Casper *Friendly Finality Gadget* (FFG), invented by Vitalik Buterin, is a hybrid PoW/PoS consensus mechanism. The protocol is implemented first to ease the transformation to a complete PoS based Ethereum planned for the Serenity stage. The design implementation of Casper FFG describes a PoS mechanism running on top of the current PoW Ethash mechanism, a so-called hybrid PoW/PoS consensus mechanism. A PoS network of validators assesses finality after every 50th block mined by PoW. After this assessment, a chain is validated as the correct PoW chain. The first implementation of Casper, Casper FFG is thus not increasing the scalability of Ethereum, but the Level of Trust and more specifically a higher level of finality will be reached (Buterin & Griffith, Casper the Friendly Finality Gadget, 2017). If Casper FFG has proven its working, Ethereum can implement Casper CBC.

The final version of Casper *Correct by Construction* (CBC), will replace the current PoW mechanism within Casper FFG into something more efficient. The PoS mechanism proposed for Casper is a BFT PoS mechanism that can be classified as a by-block consensus mechanism (Buterin, Understanding Serenity, Part 2: Casper, 2015). The opposite of by-block consensus is chain-based consensus that is specified by the longest chain in current PoW mechanism. By-block consensus means that there is consensus over each block generated, that also leads to higher level of finality for each block. On several Reddit forums, developers are speculating that Casper CBC potentially creates a three times scalability improvement on Ethereum (Reddit, 2018). The release date for Casper CBC is currently unknown.

Sharding

In current blockchains, each full node or validator (miner) has to store the complete database and process each transaction. This ensures a high level of trust; however, it limits the level of scalability. The network can be as fast as the slowest full node or validator (Buterin, Ethereum Wiki / Sharding FAQ, 2018). The idea of sharding is to split the blockchain in multiple shard-chains that all have their own set of low-level single-shard nodes. This creates smaller blockchain shards easier to manage for normal computer devices. According to Buterin (Ethereum Wiki / Sharding FAQ, 2018), There are four hierarchical node levels that validate a sharded blockchain:

- *Super-full node:* This type of node downloads the complete chain including all shards. This node should validate everything.
- *Top-level node:* This type of node validates all main-chain blocks, and has light client access to all shards. It can still check whether a new transaction is valid in all shards.
- *Single-shard node:* This type of node acts like a top-level node, but also downloads a complete shard-chain and can validate blocks on that chain.
- *Light-node:* This type of node works like a current light client, and only verifies all block headers and main-chain blocks.

According to O'Leary (2018), the sharding roadmap focussing developers to work on a minimal sharding product was finished in January 2018; however, the implementation data for this is currently unknown. Buterin announced at a conference in Taipei at the 25th of November 2017 that Ethereum should be able to scale to 1500 transactions per seconds by combining Casper, sharding and several other protocols within three to five years (Buterin, BeyondBlock Taipei, 2017).

Plasma

First of all Plasma is not an Ethereum protocol implementation like sharding or Casper, however Plasma is a design pattern or a technique that can be used to build a scalable solution on top of Ethereum

(Konstantopoulos, 2018). Plasma can be interpreted as a side-chain with a single proof of authority, called the Plasma operator. The main security mechanism is “Plasma Exit” in which a user is always allowed to exit the plasma contract. If a plasma operator becomes malicious, the plasma user has two weeks to proof that he or she owns the amount of plasma tokens, i.e. by a Merkle proof of the plasma-chain, and claim his plasma tokens back and exit the contract. The plasma operator has thus a limited amount of power over the plasma-chain. The plasma-chain is backed by the plasma contract that is a smart contract on the main-chain. The plasma operator stores the Merkle tree root hashes of the plasma-chain in the plasma contract to create immutability in the plasma-chain. If a user wants to buy some Plasma Ether, the user locks an equal amount of Ether into the plasma contract. Plasma enables fast transactions, since it can be considered as an off-chain protocol only writing small amount of data, the Merkle tree root hashes, into the plasma contract on the main-chain. Bankex (2017) already did some first testing with their plasma protocol implementation on the Ethereum Rinkeby test network and reached 5000 transactions per second. However, the security of the Plasma protocol is still unclear and it is questionable when the first implementations of the plasma protocol will be announced.

5.3 Cardano

Cardano is a project established by Charles Hoskinson, who is a former member of the Ethereum Foundation. The project is named after one of the most influential mathematicians of the Renaissance called Gerolamo Cardano. The cryptocurrency running on the Cardano blockchain is called ADA. The smallest unit is one-millionth unit of ADA and this is called a Lovelace. ADA Lovelace was the first computer programmer, and this is a tribute to him (Store of Value, 2018). The project is currently let by three institutions that all three have distinctive roles (Cardano foundation, 2018), namely the Cardano foundation, *Input Output Hong Kong* (IOHK) and Emurgo. The Cardano Foundation is a Swiss non-profit institution, that collaboratively work together with governments to "standardise, protect and promote" the Cardano technology. IOHK is an engineering company created by Charles Hoskinson and Jeremy Wood that builds blockchain solutions for academic institutions, governments and corporations. Two-mayor projects of IOHK are Cardano and Ethereum Classic. Cardano is a project completely built from scratch, which began in 2015 as an effort to create a blockchain project fully evolved out of scientific philosophy (Buchko, 2017). Despite starting with a comprehensive roadmap or whitepaper, the project started with determining a set of design principles, engineering best practices, and places still needed to be explored (IOHK, 2018). Besides the project Cardano, IOHK is also working on Ethereum Classic. Ethereum Classic started after the DAO fork of Ethereum described in chapter 1.2.2. During this fork, there was a disagreement within the Ethereum community leading to a split into Ethereum and Ethereum Classic. According to IOHK (2018), "Ethereum Classic is a continuation of the original Ethereum blockchain – the classic version preserving untampered history. Free from any external interference". Emurgo is a Venture Capital Company and its role is to speed up the adoption process of the Cardano platform for commercial applications (Cardano foundation, 2018).

According to IOHK (2018), the Cardano roadmap consists of multiple phases. Currently Cardano is at the Byron phase, which is expressed as the bootstrap era. Bootstrapping in computer science means the process of loading a set of instructions into the system as a computer boots up (Techopedia, 2018). This means that Cardano is at the early implementation phase. Table 5.8 shows the planned phases in the roadmap of Cardano and the focus of each project phase. Cardano claims to become a smart contract platform comparable to Ethereum, where ecosystems can be built upon. However, there are some differences between both. The biggest difference is the layered architecture of Cardano. Ethereum is a platform for value and computation on a single layered architecture. Cardano will be programmed as a multiple layered architecture (Buchko, 2017). Despite this difference, multiple other differences are listed in the philosophy statement of Cardano (Cardano.org, 2018). The philosophy statements of Cardano are placed in Appendix VI.

Table 5.8 Cardano roadmap. Derived from IOHK (2018)

Phase:	Focussing on:	Implementation:
Byron	Currently, Cardano is in the Byron or Bootstrap phase. Much of the work for this phase is on the networking layer and Ouroboros. This phase enables transactions, trading and purchasing of the ADA tokens on the settlement layer of Cardano.	Current phase
Shelley	This phase ensures that the technology required for the decentralization of the settlement layer and the corresponding ADA token will be finished.	Not yet implemented, planned for Q2 – Q3 2018
Goguen	This phase will implement smart contract functionality. Smart contracts on Cardano are executed by the IELE. The IELE is a virtual machine with a universal language framework for executing quasi-Turing complete smart contracts. This IELE runs on the computation layer that exists on top of the settlement layer.	Not yet, Goguen test-net planned for July 2018
Basho	This phase will focus on increasing performance, security and scalability. A revised network layer and another consensus mechanism *Ouroboros Praos* will achieve these improvements.	Not implemented
Voltaire	This phase will focus on the assurance of the network and on scalability. Additionally, the treasure model will be implemented during this phase.	Not implemented

Since Cardano is currently in the bootstrap phase, many parts of Cardano are not finished yet. Additionally, there is not much peer reviewed literature describing the current progress of Cardano

except the papers and documents from the Cardano stakeholders themselves. Therefore, the upcoming chapters represent the current state of technology. The Roadmap section provides a more elaborated version of the future vision of Cardano in which they explain their approach of solving the current problems of public blockchain technologies. At the time of writing (June 2018), the validity of the Cardano case study could be biased since there is not much information available besides the information of the Cardano stakeholders themselves. The stakeholders could have incentives to bias information to influence cryptocurrency prices.

5.3.1 Technology characteristics

The blockchain technology that drives the Cardano platform can be described as a set of technology characteristics. These technology characteristics include a set of IDCs and a set of CPs. The CPs are built on top of the Cardano blockchain to improve the service characteristics of Cardano. The CPs services on top of the Cardano are left out of scope, since the data available for Cardano is scarce and Cardano is still in the Byron phase (Table 5.8). Table 5.9 provides an overview of the technology characteristics of Cardano derived from a variety of sources. The upcoming subchapters provide an overview of the different technology characteristics.

Table 5.9 Cardano technology characteristics

	Technology characteristic:	**sub-characteristic:**	**Cardano' s implementation:**
IDC	*Network design*		Distributed (Peer-to-Peer)
	Consensus mechanism		Delegated PoS with 7 fixed nodes
	State machine architecture	Coding language	Haskell (functional programming language)
		Smart contract execution	Not implemented yet
		Data structure	Transaction-based (UTXO)

Network Design

Currently, Cardano has only implemented the settlement layer. The protocol responsible for the network structure is the Kademlia Distributed Hash Table open peer-to-peer protocol (Cardano Docs, 2018). The properties of the peer-to-peer protocol are comparable with Ethereum, since both protocols are based on the Kademlia algorithm. Additionally, BitTorrent also uses the Kademlia algorithm. Therefore, the current network design of the settlement layer is characterised as a distributed Peer-to-peer network.

Consensus Mechanism

On top of the distributed settlement layer of Cardano runs the consensus mechanism of Cardano. The consensus mechanism can be characterised as an internal design consideration to reach consensus about the state of the ledger. A general explanation of the PoS consensus mechanism is elaborated in chapter 2.2.4. The consensus mechanism is a PoS based mechanism called Ouroboros. "Ouroboros is unique as it is the first blockchain protocol that is based on PoS and has been scientifically proven as secure" (Cardanodocs, 2018). However, the security of this protocol is doubted by others (Larimer, 2018). The Ouroboros PoS mechanism divides the blockchain into epochs. Each epoch is split into a set of slots. A random generator is used as selection mechanism to select the slot leaders. A single slot last 20 seconds and during this time a slot leader has the opportunity to create and add a new block to the slot (Allison, 2018). Since Cardano is currently at the Byron phase, Ouroboros is not finally implicated yet. The current consensus mechanism is called *delegated Proof of Stake* (DPoS), which means that only a fixed set of seven nodes can validate the network. This means that the current implementation of the consensus mechanism is arguably centralized and the seven nodes have control over the network. The community claims that this is required in order to maintain security over the network during this phase of Cardano (Store of Value, 2018).

Layered State machine architecture

The architecture running on top of the consensus mechanism is the state machine. The final version of Cardano can be considered as multi-layered state machine consisting of the *Cardano Computation Layer* (CCL) and the *Cardano Settlement Layer* (CSL). This separates the accounting and the computation into two different blockchains. The design is borrowed from TCP/IP in order to separate the elements of concerns (Whycardano.com, 2018). Both blockchain layers are allowed to communicate to each other by sidechains. The benefit of this layered architecture is a more flexible system that enables different government mechanisms and different security solutions for the different chains (Store of Value, 2018). The lower CCL layer is defined as the layer where the value is stored, while the CSL layer performs the calculations. Therefore, the CCL layer should be very secure while the CSL layer allows a lower security level. Since Cardano is currently in the Byron phase, currently only the CSL is available on the Cardano main network.

Equal to bitcoin, the CSL blockchain uses the UTXO transaction data structure (CardanoDocs, 2018). The explanation of the UTXO transaction model is elaborated in chapter 5.1.1. Additionally, Smart contracts are currently not available on Cardano main net since the CCL is not finished. Smart contracts functionality will be implemented in the Goguen phase and is introduced by the implementation of the IELE virtual machine. The IELE is currently not implemented and therefore the working is left out of scope.

One important technical characteristic of the CCL layer is that it is programmed with Haskell computer code (IOHK, 2018). Haskell is a programming language that unlike C, C++, and Java is a pure functional programming language. This type of programming languages is strong and statically formulated and does not allow typographical errors. Since functional computer code is much easier to validate mathematically, it is much easier to prove the exact input and output of a program. Due to this characteristic, Cardano claims to become a cryptocurrency with a very high degree of fault tolerance (whycardano.com, 2018), and Cardano gets the “High Assurance Code” property (Rosic, What is Cardano Blockchain? Step-by-Step Guide, 2018). Appendix VI shows a table describing the general differences between imperative and functional programming.

5.3.2 Service characteristics

The services delivered by Cardano can be described as a set of service characteristics. Table 5.10 provides an overview of these service characteristics, which are further elaborated in the upcoming subchapters. The validity of the Cardano case study could be biased since there is not much information available regardless the information of the Cardano stakeholders themselves.

Table 5.10 Cardano service characteristics

Service characteristic:	**sub-characteristic:**	**Current level:**
Functionality	Native functionalities	Cryptocurrency ADA
Level of Privacy	User level privacy	Pseudonymous
	Transaction level confidentiality	Open and accessible
Level of Trust	Security	Unknown
	Finality	Unknown
	Liveness	Unknown
Level of Interoperability		(currently) Poor
Level of scalability	Maximum throughput	10-15 TX/sec (Store of Value, 2018)
	Latency	20 seconds (Larimer, 2018)
	Transaction costs	Pay per byte: ~$0,034 at 31-5-18
Governance		Currently centralized governance

Functionality

Since Cardano has only implemented the CSL layer, the only native functionality currently is the ADA cryptocurrency. ADA is the main functionality of CSL. Similar to bitcoin, ADA can be defined as a Cryptocurrency and Spenkelink (2014) defines cryptocurrency as "a digital medium of exchange that relies on a decentralized network that facilitates a peer-to-peer exchange of transactions secured by public key cryptography". However, currently Cardano is not a truly decentralized network since the consensus protocol seems centralized. The centralization challenge will be solved in the next phase of the roadmap; Shelley, that enables a transition towards a truly decentralized cryptocurrency (IOHK, 2018).

Level of Privacy

Currently the level of privacy characteristic of CSL layer is equal to bitcoin. The accounts on the CSL layer are pseudonymous and the transactions are open and accessible (Cardanodocs, 2018). Cardano has several ideas on the roadmap to improve the level of privacy service characteristic and these are mentioned in chapter 5.3.4.

Level of Trust

This research has argued that on Bitcoin and Ethereum the level of trust service characteristic is related to the consensus mechanism characteristic. Since the current implementation of Ouroboros consensus mechanism currently only has seven nodes, the level of trust characteristic of Cardano is arguable poor. It simply means that all stakeholders of Cardano have to trust the integrity of these seven nodes. Larimer (2018) describes another trust issue within Cardano. He argues that it takes up to 5 hours to get a decent amount of finality for single transaction. It should be noted that the validity of this claim is unclear. On this moment, no validation measures from independent stakeholders regarding the trust of Cardano can be found in literature. Therefore, the current level of trust is set at unknown. Cardano has to prove over time that the network is trustworthy.

Level of Interoperability

Similar to Bitcoin and Ethereum, the level of Interoperability of Cardano is considered poor since the protocol itself does not support direct communication with other blockchains. Cardano has several ideas on the roadmap to improve the level of interoperability characteristic and these are mentioned in chapter 5.3.4.

Level of Scalability

Similar to Bitcoin and Ethereum, the level of scalability is an important challenge for Cardano. According to their roadmap, scalability is an important issue that will be solved during the Basho and Voltaire phase (IOHK, 2018). The scalability measure of Cardano is hard to quantify since validated information is scarce. Equal to Bitcoin and Ethereum, this subchapter treats the maximum throughput, the latency and the CPCT of the Cardano platform as level of scalability metrics. These metrics are obtained and is validated wherever possible; however, the validity of these metrics could be biased since there is not much information available except the information of the Cardano stakeholders themselves.

Maximum throughput

Not much data is available to measure the maximum throughput of Cardano. According to a presentation from Duncan Coutts seven months ago, Cardano currently has an average transaction throughput between 10 – 15 transactions per second (Cardano Reddit, 2018). This seems to be slower than Ethereum, however the 31.66 represents the maximum throughput for the most simplistic transactions on Ethereum. Overall, it is not possible to make proper claims about the throughput of Cardano since the required data is not available in literature and quantitatively measuring it is out of scope.

Latency

The time to obtain a single confirmation within Cardano is currently 20 seconds and is related to the targeted slot time of 20 seconds (Larimer, 2018). This rule only applies for an uncongested network where the transaction comes with a decent amount of fee that incentivises miners to include the transaction in a block.

Cost per Confirmed Transaction (CPCT)

According to Croman et al. (2016), CPCT encompasses several distinct resources to keep the Bitcoin network running and secure. The CPCT of Cardano will be slightly different and can be explained as operation cost, which are mainly bandwidth cost since the energy costs are negligible in PoS, and capital equipment costs including:

- *Staking costs:* The loss of potential value increases due to inflation or deflation for the staked cryptocurrency in relation to other currencies.
- *Computation validation (gas) costs:* The cost that is spent to perform the required computation for the validation of a transaction.
- *Bandwidth costs:* The cost of network resources to keep the network in sync including all transactions, the blocks and the metadata.
- *Storage costs:* The cost of storing the complete blockchain, which is required for each full node and each miner.

It is very hard to measure these metrics, since cryptocurrency prices, amount of transactions per second, and hardware prices continuously fluctuate. The cost per confirmed transaction of Cardano cannot be found in literature, but is considered lower than Bitcoin and Ethereum CPCT, since the Cardano network is more efficient and does not require PoW. Similar to Ethereum, Cardano will become a smart contract platform that is not specifically made for ADA transactions and therefore, the cost per confirmed computation is a better metric for Cardano. According to Cardanodocs.com (2018), the current transaction fees in Cardano are calculated by the following equation:

$$a + b * size \quad \textbf{(1)}$$

In which:

- a is a fixed constant, currently set at 0.155381 ADA;
- b is multiplier constant, currently set at 0.000043946 ADA/byte;
- size is the size of the transaction in bytes.

A typical size for a simple transaction is 200 byte, and one transaction thus cost ~0.164 ADA (CardanoDocs, 2018). According to CoinMarketCap (2018), the price of one unit of ADA is ~$0,21 on the 31th of May 2018. This means that a simple transaction on Cardano costs ~$0,034, which is much cheaper than a single Ethereum or Bitcoin transaction. Arguably, the reason for this price difference is the centralized network of only 7 validating nodes, and the PoS implementation which is much more energy efficient.

Governance

Not much data is available about the current way of governance in Cardano. Three institutions called the Cardano foundation, IOHK and Emurgo, currently lead and influence Cardano. Additionally, the seven DPoS validating nodes are in control by these three institutions to ensure a stable and secure network (Cardanodocs, 2018). The institutions have full control over what happens within the network. This is different for Bitcoin and Ethereum where the communities do not have full control over the blockchain. Therefore, this research concludes that Cardano is currently governed in a centralized way.

Cardano has interesting ideas of changing governance in the future, and these are elaborated in the Roadmap chapter.

5.3.3 Cardano characterisation framework

Table 5.11 shows the characterisation model of Ethereum derived from empirical research. The model describes the service characteristics, the technology characteristics of the Cardano platform.

Table 5.11 Cardano as a set of service and technology characteristics

Services characteristics		
Current level	*sub-characteristic*	*main-characteristic*
Cryptocurrency ADA	Native functionalities	**Functionality**
Pseudonymous	User level privacy	**Level of Privacy**
Open and accessible	Transaction level confidentiality	
Unknown	Security	**Level of Trust**
Unknown	Finality	
Unknown	Liveness	
(currently) poor		**Level of Interoperability**
10-15 TX/sec	Maximum throughput	**Level of scalability**
~20 seconds	Latency	
Pay per byte: ~$0,034 at 31-05-18.	Transaction costs	
Currently centralized governance		**Governance**

Technology characteristics		
main-characteristic	*sub-characteristic*	*implementation*
Network design		*Distributed (Peer-to-Peer)*
Consensus mechanism		*Delegated PoS with 7 fixed nodes*
State machine architecture	Coding language	*Haskell (functional programming language)*
	Smart contract execution	*Not implemented yet*
	Data structure	*Transaction-based (UTXO)*

From this case study, it can be concluded that Cardano is currently not matured and is still in early implementation phase. Additionally the platform currently has many challenges. Only the CSL is working with a centralized consensus and governance mechanism. The interesting part of Cardano is how they will solve the current issues in the blockchain technology landscape. The upcoming chapter elaborates on the future vision of Cardano and founder Charles Hoskinson.

5.3.4 Roadmap

According to Hoskinson (2017) who founded Cardano, there are currently three generations blockchains. Generation 1.0 stands for the single use case cryptocurrency blockchain for which Bitcoin is an example. Generation 2.0 stands for a blockchain platform that can run smart contracts for which Ethereum is an example. These definitions correspond to the Generation 1.0 and 2.0 definitions defined provided by Swan (2015), which are treated in chapter 1.1.2. Within the first two generations, Hoskinson found several issues and claimed that Cardano will solve these issues. Therefore, Hoskinson claimed that Cardano would become a generation 3.0 blockchain. The challenges that Cardano is solving to become generation 3.0 are related three elements, which are Scalability, Interoperability and Sustainability. Cardano also create a clear philosophy in which they explain their design choices. This philosophy is listed in Appendix VI. The upcoming subchapters elaborate on the three elements that Cardano will implement in the upcoming years.

Scalability within Cardano

Hoskinson (2017) described three separate elements that are important for scalability within Cardano, which are throughput, network and data scaling.

The first element described by Hoskinson (2017) is throughput. As concluded in the Ethereum and Bitcoin case study, throughput is currently a challenge for public blockchain technologies. This is partly due to the PoW consensus mechanism. From start, Cardano has implemented their version of DPoS, called Ouroboros. The current version of Ouroboros is centralized with only seven validating nodes. Cardano has the vision to solve the throughput challenge of blockchains with a different consensus mechanism in the format of an efficient academically validated DPoS mechanism. The decentralized version of Ouroboros is scheduled for the Shelley phase and the more scalable Ouroboros Praos is scheduled for the Basho phase (IOHK, 2018).

Another scalability element addressed by Hoskinson (2017) is network. The challenge network is explained as bandwidth of a decentralized network. Hoskinson argues that transactions carry data, and if the amounts of transactions grow, the network requires more bandwidth. Within a homogenous network topology, each node relays each transaction and processes all data. In this topology, the bandwidth is limited towards the slowest node. Cardano will solve this by implementing another type of network topology, called *Recursive Inter Network Architecture* (RINA). “Rina is a new type of structuring networks using policies and ingenious engineering principles” (Rosic, What is Cardano Blockchain? Step-by-Step Guide, 2018). Cardano promises that RINA will solve the following challenges: privacy, transparency and scalability. RINA is a method of splitting the network in multiple parts and each node is designated to its own part. Therefore, RINA in Cardano is somehow comparable with sharding of Ethereum.

The third element addressed for scalability is data scaling. Since blockchains are considered immutable and each node stores a full copy of the blockchain, the blockchain size becomes an increasing challenge for each node. Cardano thinks about pruning, subscriptions and compression of data to decrease the required storage requirements for a particular group of nodes. Not each node has to download the complete chain, and only has to download parts of the chain (Rosic, What is Cardano Blockchain? Step-by-Step Guide, 2018). Arguably, this property is also included in sharding of Ethereum.

Above elements are three ways of scaling the Cardano blockchain. The second challenge that Cardano is trying to solve is interoperability.

Interoperability within Cardano

Hoskinson (2017) argues that currently it is almost not possible for current blockchains to intercommunicate without third parties, i.e. the Bitcoin blockchain cannot communicate directly with Ethereum and vice versa. In case of interoperability, Cardano tries to become the “internet of blockchains”. Cardano want to enable cross-chain transfers without the requirement for a third party. Cardano aims to implement this attribute by using side-chains. According to Hoskinson (2017), a side-chain increases scalability and increases interoperability. Both characteristics are also included within the Ethereum Plasma design protocol and a plasma-chain can be considered as side-chain. If a sidechain is attached via a two-way peg with two blockchains, interoperability thus seems possible according to Hoskinson (2017). The third challenge that Cardano is trying to solve is sustainability.

Sustainability within Cardano

Hoskinson (2017) argues that the third element defining a generation three blockchain is sustainability, i.e. how will a blockchain pay for its future development, server cost or growth? Cardano aims to implement a treasury mechanism to solve these issues. The idea of a treasury mechanism comes from the Dash cryptocurrency blockchain. In current blockchains, for each block created the miner receives the block reward. Within Bitcoin, the current block reward is set at 12.5BTC. In case of a treasury mechanism, the block reward is divided in two parts, one part for the miner and the other part for the

blockchain treasury. This treasury can be used to pay for multiple costs such as future development, a blockchain service desk, or other future costs. The treasure mechanism works as follows. If somebody in the Cardano ecosystem wants to develop or add changes to the chain, that user can submit for a ballot. Afterwards, the stakeholders have to vote for ballot approval or disproval. If the ballot is approved, the applier will receive funds for the development. Rosic (2018) argues about several challenges that have to be solved for the treasury model to work:

- A proper and fair voting mechanism has to be set in place.
- The voting users should have an incentive to vote and participate otherwise problems will occur.
- Every vote should have some value; otherwise, a "tragedy of commons" type of situation could occur. Tragedy of commons describes a situation where the individual has a higher incentive to vote for its self-interest instead of voting for the communities' best interest.
- The process of proposing a ballot should be easy and straightforward.
- The entire process needs to be as decentralized as possible.

In order to fulfil above challenges, Cardano is currently working on a system called liquid democracy. Liquid democracy is a governance mechanism that enables democratic voting on-chain. According to Duncan (2017), there are many forms of implementing a democratic process on a blockchain technology. The two well-known forms are in both opposites of the spectrum and are direct democracy and representative democracy. In direct democracy, everyone has to vote and has equal voting power. In representative democracy, voting goes like a more traditional hierarchy system. According to Schiener (2015), who is one of the founders of IOTA, "Liquid Democracy combines the advantages of both direct and representative democracy and creates a truly democratic voting system that empowers voters to either vote on issues directly, or to delegate ones voting power to a trusted party". It therefore seems to be a more agile mechanism of voting. Currently, not much information is available about the technological implementation of liquid democracy.

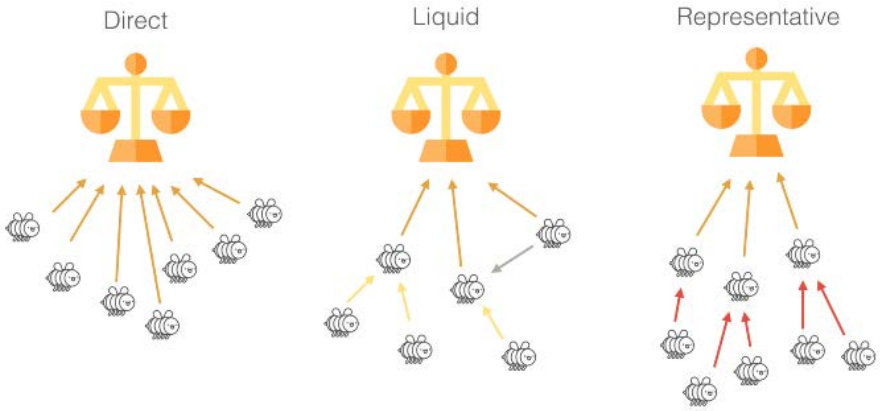


Figure 5.5 Three forms of democratic voting mechanism. Adapted from Duncan (2017).

The above-proposed elements provide a clear overview how Cardano will solve the current issues of public blockchain technologies. There is some overlap in the roadmaps of Cardano and Ethereum and several basic characteristics proposed by both communities show some overlap. The upcoming result chapter will elaborate about these overlaps.

5.4 Results discussion

This chapter contains the result and lessons learned from the multiple case study.

5.4.1 Blockchain qualification framework

Chapter 4 describes the initial conceptual model based on Saviotti & Metcalfe (1984) ideology describing a blockchain technology as two sets of service and technology characteristics that are interlinked by a pattern of mapping. During the case study, this model slightly changed, and finally the model is validated by several semi-structured interviews. This chapter will introduce the missing pattern of mapping. The pattern of mapping is composed using the findings of the case study and the semi-structured interviews. Table 5.12 shows the introduced framework that can be used for qualification of public permissionless blockchain technologies.

Table 5.12 A characterisation framework for public permissionless blockchains

Services characteristics	
sub-characteristic	*main-characteristic*
Native functionalities	**Functionality**
Add-on functionalities	
User level privacy	**Level of Privacy**
Transaction level confidentiality	
Security	**Level of Trust**
Finality	
Liveness	
	Level of Interoperability
Maximum throughput	**Level of scalability**
Latency	
Transaction costs	
Incentives	**Governance**
Mechanism for Coordination	

Technology characteristics	
main-characteristic	*sub-characteristic*
Network design	
Consensus mechanism	
State machine architecture	Coding language
	Smart contract execution
	Data structure
	Block size
	Block release time
	Block header data structure
Complementary protocols	interchain protocol
	offchain protocol

The upcoming subchapters provide a summarized explanation of the pattern of mapping interlinking the service characteristic with the technology characteristics. The findings are backed by the multiple case study.

Functionality

The functionality characteristic is linked to the state machine architecture. In Ethereum, the EVM is capable of running quasi-Turing complete scripts and this drastically extends the functionality of the platform. The EVM is part of the state machine architecture.

Level of Privacy

The level of privacy characteristic is linked to state machine architecture and the complementary protocol characteristics. In Ethereum, zkSNARKs is already implemented in the state machine. This potentially increases the transaction confidentially. Additionally, complementary protocol off-chain solutions such as Lightning and Raiden increase the level of privacy by enabling off-chain transactions that are not open and accessible by each on-chain stakeholder.

Level of Trust

The level of trust characteristic is linked to network design and consensus mechanism. As founded in the case study, the consensus mechanism is strongly related to all three sub-characteristics, security, finality and liveness.

Level of Interoperability

The level of interoperability characteristic is currently only linked to complementary protocols. A decentralized exchange is a type of complementary protocol and can increase the level of interoperability. Currently, state machine architecture is not linked to the level of interoperability since there is no native support by the three researched cases for on-chain interoperability protocols.

Level of Scalability

The level of scalability characteristic is linked to consensus mechanism, state machine architecture and complementary protocols. The shift towards Casper CBC, which is the second-generation Casper PoS consensus mechanism, enables a higher level of scalability for Ethereum. Additionally, a transition towards a more efficient EVM, potentially eWASM, which is excluded from this research, would lead to a higher level of scalability (eWASM GitHub, 2018). Additionally, the proposed sharding solution of Ethereum can be characterised as a mix of consensus and state machine improvements. Sharding will increase the level of scalability of Ethereum. Furthermore, complementary protocols such as Lightning and Raiden will contribute to a higher level of scalability.

Governance

The governance characteristic is linked to consensus mechanism and additionally to off-chain mechanism. On-chain governance is currently only implemented by Ethereum related to gas block limit voting and by bitcoin in signalling (miners voting) on protocol upgrades. Off-chain government solutions are not linked to the technology characteristics. On-chain governance can be included by multiple voting solutions. Voting is a method of reaching consensus within a group of users. Therefore, Consensus mechanisms can potentially include voting technology enabling on-chain governance in the future.

5.4.2 Challenges and solutions for public permissionless blockchain technologies

The case study identified several challenges within pubic permissionless blockchain technologies. The challenge regarding the low functionality of Bitcoin (generation one) is solved by Ethereum (generation two) that included smart contracts functionality and a quasi-Turing complete virtual machine. Currently generation two have several challenges. A summarized list of blockchain challenges identified during the research is provided below. The case study provides a more a more detailed overview.

- *Level of Privacy:* The level of privacy is a challenge for public permissionless blockchain technologies. Users currently do not possess user account privacy and transaction level confidentiality is scarce. Several protocols are currently investigated to improve the level of transaction confidentiality, e.g. zkSNARKs.
- *Level of Trust:* Although the level of trust is considered high for Bitcoin and Ethereum, both protocols do not enable absolute finality, which is required for some use cases. This challenge relates to the current PoW consensus mechanism implementation. The PoS consensus mechanism that is proposed by the Ethereum community, Casper FFG and Casper CBC, would potentially increase finality for Ethereum.
- *Level of Interoperability:* Currently, the three studied blockchain technologies do not enable native interoperability solutions. Interoperability is a problem not only for blockchain, but also for many other computation cloud platforms (Foster, Zhao, Raicu, & Lu, 2008). Currently the proposed solutions are mostly complementary protocols, i.e. side-chains, which enable a mechanism for interoperability between two blockchain platforms.

- *Level of Scalability:* One of the most debated issues is scalability. Public blockchains currently have low throughput and high CPCT. This is the trade-off for decentralized computations. Currently, several technology solutions are proposed that potentially increase the level of scalability (Table 5.13).
- *Governance:* Governance can be split ifn off-chain and on-chain governance. Currently, much of the governance occurs off-chain by a selected group of participants. A truly democratic system would be in place where each stakeholder has equal voting rights. Such as system is very complex and brings multiple challenges. A solution opposed for on-chain delegated voting is the liquid democracy model however, this solutions seems far from integration. Another large governance problem for blockchain use cases is that the price of the system cannot be predicted due to cryptocurrency price fluctuations. Overall, the governance service characteristic brings many challenges to public permissionless blockchain technologies.

Table 5.13 shows a list of proposed technology solutions that potentially solves several of the current challenges. The table also includes the links of technology and service characteristics. The table shows that the communities are very reserved in providing dates for potential protocol upgrade. Additionally, Cardano seems to have many solutions for current challenges; however, based on their current achievements they have a long path to go to become what they claim to be a generation three blockchain.

Table 5.13 List of proposed solutions concluded from the case study

Technology solution:	**Platform:**	**Technology characteristic:**	**improved (+) or reduced (-) service characteristic:**	**Date of arrival (N.D.A means no date available)**
Lightning networks	Bitcoin	Complementary protocols / Off-chain protocol	Level of Privacy/ transaction level confidentiality +, Level of Interoperability +, Level of Scalability +	Currently available in beta phase, Release candidate 06-12-17
Raiden networks	Ethereum	Complementary protocols / Off-chain protocol	Level of Privacy / transaction level confidentiality +, Level of Interoperability +, Level of Scalability +	Currently the MVP micro Raiden is available in beta phase, Implementation soon
Casper	Ethereum	Consensus mechanism	Level of Trust (debatable) / Finality +, Level of Scalability +, Governance -	Casper FFG mid-2018 Casper CBC N.D.A.
Sharding	Ethereum	Consensus mechanism / state machine architecture	Level of Scalability +, Governance -	N.D.A
Plasma	Ethereum	Complementary protocols / Off-chain	Level of Privacy / transaction level confidentiality +, Level of Scalability +	N.D.A
Ouroboros Praos	Cardano	Consensus mechanism	Level of Trust ? / Finality +, Level of Scalability +, Governance -	N.D.A
RINA	Cardano	Consensus mechanism / state machine architecture	Level of Scalability +, Governance -	N.D.A
Treasury model	Cardano	Consensus mechanism	Governance +	N.D.A
Liquid democracy model	Cardano	Consensus mechanism	Governance +	N.D.A

6 Conclusion

The upcoming subchapters describe the conclusions of this research. Firstly, an answer is provided for the sub research questions of this research. Secondly, the main research question is answered. Thirdly, suggestions for future research are provided from the researcher point of view, and fourthly the validity of this research is discussed.

6.1 Sub questions

The first sub question addressed by this research is *'How to characterise public permissionless blockchain technologies?'*

The answer of this question is provided in the format of a characterisation framework based on Saviotti & Metcalfe (1984) ideology describing a technology as two sets of service and technology characteristics that are interlinked by a pattern of mapping. This model can be used in order to qualify the innovation output of public permissionless blockchain technologies. The identified main service characteristics are; Functionality, Level of Privacy, Level of Trust, Level of Interoperability, Level of Scalability and Governance. The identified main technology characteristics are; Network design, Consensus mechanism, State machine architecture and Complementary protocols. The sets of service and technology characteristics are interlinked by a pattern of mapping. Additionally, each main characteristic is if appropriate subdivided in a set of sub-characteristics. Table 5.12 shows the introduced public permissionless blockchain characterisation framework.

The second sub question addressed by this research is *'What are the essential design considerations in the selection of a public permissionless blockchain technology for business use cases?'*

The framework introduced for the first sub question can also be interpreted as a guideline to define the technology design considerations. It should be noted that the framework only applies to the design choices regarding the selection of a technology. The set of service characteristics can help defining the technology requirements for a blockchain use case. If the requirements are set, the pattern of mapping provides assistance in selecting the right set of technology characteristics specific to a blockchain technology. The knowledge acquired from the interviews and the TCB platform meetings have provided the insight that the technology behind blockchain is only a small part of a blockchain use case. Many other decisions required for a use case, such as Legal in relation to GDPR, the governance and questions like 'who is responsible?' are as important as the technology decision. Appendix IV describes that blockchain as a physical technology enables new forms of social technologies. These new forms of social technologies require a different mind-set for people to collaborate. People have to find new ways of mutual trusting each other using blockchain. Additionally, off-chain governance and legal aspects require much attention for blockchain use cases. Public permissionless blockchain technologies only work if people start collaborating in new forms. For businesses, this implies that new business models have to be explored that enable new types of collaboration.

The third sub question addressed by this research is *'What are the current challenges within public permissionless blockchain technology platforms and how will the blockchain communities solve these challenges?'*

The results of the case study identified five challenges for generation two public permissionless blockchains; namely, Level of Privacy, Level of Trust, Level of Interoperability, Level of Scalability and Governance. The first generation cryptocurrency also has functionality as challenge since this characteristic of generation one blockchain is limited. Chapter 5.4.2 provides an overview of the challenges of public permissionless blockchain technologies. It should be noted that each use case requires a different set of service characteristics and therefore, not all five challenges are applicable for each use case. Each use case should identify its own set of service characteristic requirements. Although public permissionless blockchains have serious challenges, the open source communities are currently

putting much effort in solving the technology challenges. An overview of the solutions is provided in Table 5.13. For most solutions, the date of arrival for future upgrades is unclear since the communities are very reserved in providing dates. It should be highlighted that the blockchain communities have a clear vision on how they will solve the current challenges. This vision is comparable to a roadmap, and is used by the open source communities to steer developments for the platform. This is also mentioned in the roadmap literature review, where open source communities use roadmapping as a method to reach community consensus about their R&D efforts.

6.2 Main research question

The main research question addressed by this research is *'How to qualify public permissionless blockchain technologies and why are these not wide-scale adopted for business use cases?'*

Blockchain technology is a digital platform top trend in the Gartner hype cycle of 2017 (Panetta, 2017). This suggests that blockchain is currently in a hype; however, production ready public permissionless blockchain use cases are scarce. Several reasons for this are identified. Firstly, current public permissionless blockchain technologies have many technical challenges and these challenges are mentioned in chapter 5.4. Currently, the open source communities are putting much effort in solving the technological challenges and therefore this research strongly recommends companies to follow the developments regarding public permissionless blockchains closely in order to not miss the boat. Secondly, public permissionless blockchain technologies have a high level of trust, are decentralized and are secure; this has trade-offs for scalability. Therefore, the technology solution design of blockchain use cases should be as minimalistic and efficient as possible. Thirdly, the technology behind blockchain is only a small part of a blockchain use case. Many other decisions required for a business use case introduce many other (non-technical) challenges, such as legal in relation to the general data protection regulation (GDPR), compliance and off-chain governance. Questions like 'who is responsible?' and regarding the price volatility of cryptocurrency often occur and have to be solved. Fourthly, blockchain technology enables new forms of collaboration between people and businesses and this sometimes feels scary, this implies that new business models have to be explored that enable new types of collaborations. Besides the challenges, public permissionless blockchains create many opportunities regarding new or more efficient business models. It should be noted that corporates are currently investigating many public permissioned blockchains and corresponding use cases. During the research, Rabobank went live with the we.trade platform, which is a private permissioned blockchain platform based on Hyperledger Fabric.

6.3 Suggestions for future research

Many forms of future research are possible and recommended since blockchain technology is still in infancy. This research provided an overview of the current state of technology and challenges for the technology regarding public permissionless blockchains. Additionally, the research suggests looking through the hype of blockchain technology. Building upon the information gathered in this research, a more business-focussed research describing the challenges from a business point of view would be interesting. Furthermore, a research using the framework of Saviotti & Metcalfe (1984) describing the characteristics of public permissioned, private permissioned blockchains and other types of DLTs would be very interesting. Additionally, governance for public permissionless blockchains is an unattended problem that is very hard to solve with current technology solutions. More research towards new forms of governance mechanism, both on-chain as well as off-chain is strongly recommended, as well as more validation for the cryptoeconomics field. Cryptoeconomics is a very interesting and novel field that is currently unaddressed in the academic world. This field provides a novel and interesting mechanism of analysing economic incentives in relation to cryptography. Cryptoeconomics can potentially bring new economical mechanism how to incentivize human behaviour in relation to cryptography and information technology. Therefore, the potential is massive.

6.4 Validity of the research

This research does not predict the future, although it provides an overview the potential upgrades for the future. This subchapter assesses the validity of the findings and the reliability of the approach used in this study.

6.4.1 Qualitative validity

“Validity is one of the strengths of qualitative research and is based on determining whether the findings are accurate from the standpoint of the researcher, the participant, or the readers of an account” (Creswell, 2014, p. 251). A member of the Innovation sciences department of the Technical University of Eindhoven has conducted this research at the Blockchain Acceleration Lab from Rabobank Utrecht. This could potentially shape the interpretation of the blockchain theory. This study uses the several sources of information since unbiased academic literature is scarce due to the infancy phase of the technology. The validity of the information is debatable, but checked where possible. The validity of the conclusions is checked by multiple unstructured and semi-structured interviews and a presentation including a discussion at the Blockchain innovation week in The Hague. Besides the unstructured interviews, only four semi-structured interviews are conducted for this research and these could be biased. The outcomes of the interviews are validated where possible. Regarding triangulation, many different data source are used to acquire information to answer the RQ. The information comes from variety of people using interview methods, participating on developer forums and visiting multiple conferences and TCB meeting.

6.4.2 Qualitative reliability

Since there is not much academic validated research in the area of public permissionless blockchain, the reliability of this research is debatable. However, many different sources of information are used and experts are approached in order to guarantee the reliability of this study.

6.4.3 Limitations framework & method

Saviotti and Metcalfe (1984) have described a framework to analyse the evolution of a technology. This framework is used to describe a blockchain technology as two sets of service and technology characteristics that are interlinked by a pattern of mapping. In literature, the framework uses quantitative methods to quantify the characteristics of a technology. A quantitative method regarding blockchain technology is not possible since the technology is currently in infancy. Methods such as patent analysis are not possible, and unbiased academic literature is scarce regarding public permissionless blockchains. The research provides an example that the framework is also usable for qualifying the characteristics of a technology.

7 References

0xcert. (2018, may 2). *Beyond CryptoKitties: ERC721 non-funigble tokens on blockchain explained.* Retrieved from medium.com: https://medium.com/@0xcert/beyond-cryptokitties-erc721-non-fungible-tokens-on-blockchain-explained-30f7f7b44a19

Akentiev, A. (2017, November 8). *Parity Multisig Hacked. Again.* Retrieved from medium.com: https://medium.com/chain-cloud-company-blog/parity-multisig-hack-again-b46771eaa838

Allan, A., Edenfeld, D., Joyner Jr., W. H., Kahng, A. B., Rodgers, M., & Zorian, Y. (2002). 2001 Technology Roadmap for Semiconductors. *Computer*, 42-53.

Allison, I. (2018, March 4). *Cardano: The nitty-gritty of next generation blockchains.* Retrieved from ibtimes.co.uk: https://www.ibtimes.co.uk/cardano-nitty-gritty-next-generation-blockchains-1664909

Alyson. (2014, December 29). *Drawing the distinction between the uppercase "B" and lowercase "b" in Bitcoin.* Retrieved from Blockchain Blog: https://blog.blockchain.com/2014/12/29/drawing-the-distinction-between-the-uppercase-b-and-lowercase-b-in-bitcoin/

Anderson, L., Holz, R., Ponomarev, A., Rimba, P., & Weber, I. (2016). New kids on the block: an analysis of modern blockchains. *University of Sydney*, 1-14.

Antonopoulos, A. M. (2014). *Mastering Bitcoin.* Sebastopol: O'Reilly Media.

Antonopoulos, M., & Wood, G. (2018). *Mastering Ethereum.* O'Reilly Media.

Aste, T., Tasca , P., & Matteo, T. D. (2017). The Foreseeable Impacton Society and Industry. *IEEE Computer Society*, 18-28.

Atzori, M. (2015). *Blockchain Technology and Decentralized Governance: Is the state still necessary?* Cyprus: University of Nicosia.

Aumasson, J., & Jovanovic, P. (2016). *Blockchains in 2016: status quo and scaling challenges.* Cheseaux-sur-Lausanne, Switzerland: Kudelski Security.

Baars, D. (2016). *Towards Self-Sovereign Identity using Blockchain Technoloyg.* Twente: University of Twente.

Bankex. (2017, December 25). *Salvation From Cryptokitties Draws Near: Plasma AntiCataclysm.* Retrieved from blog.bankex.org: https://blog.bankex.org/salvation-from-cryptokitties-draws-near-plasma-anticataclysm-679adb2c1738

Barterdex. (2018, March 27). *Supernet.* Retrieved from barterdex.supernet.org: http://barterdex.supernet.org/

Bauerle, N. (2018, januari 26). *What are Blockchain's Issues and Limitations?* Retrieved from coindesk.com: https://www.coindesk.com/information/blockchains-issues-limitations/

BCC. (2017, December 5). *CryptoKitties craze slows down transactions on Ethereum.* Retrieved from BBC.com: http://www.bbc.com/news/technology-42237162

Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain - the gateway to trust-free cryptographic transactions. *Twenty-fourth European Conference on Information Systems (ECIS)*, (pp. 1-14). Istanbul, Turkey.

BIP GitHub. (2018, Februari 12). *BIPS.* Retrieved from GitHub: https://github.com/bitcoin/bips/blob/master/README.mediawiki

Bitcoin Wiki. (2016, July 22). *Value overflow incident.* Retrieved from bitcoinwiki.it: https://en.bitcoin.it/wiki/Value_overflow_incident

Bitcoin Wiki. (2018). *Bitcoin Improvement Proposals*. Retrieved from bitcoinwiki: https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals

Bitcoin Wiki. (2018, June 5). *Block size limit controversy*. Retrieved from Bitcoinwiki: https://en.bitcoin.it/wiki/Block_size_limit_controversy#Segregated_Witness

Bitcoin Wiki. (2018, May 12). *Controlled supply.* Retrieved from bitcoin.it: https://en.bitcoin.it/wiki/Controlled_supply

Bitcoin Wiki. (2018, June 11). *Deterministic wallet.* Retrieved from bitcoinwiki: https://en.bitcoin.it/wiki/Deterministic_wallet

Bitcoin Wiki. (2018, april 11). *Multisignature*. Retrieved from bitcoinwiki: https://en.bitcoin.it/wiki/Multisignature

Bitcoin Wiki. (2018, march 27). *Off-chain Transactions.* Retrieved from bitcoinwiki: https://en.bitcoin.it/wiki/Off-Chain_Transactions

Bitcoin Wiki. (2018, May 29). *OP_Return*. Retrieved from bitcoin.it: https://en.bitcoin.it/wiki/OP_RETURN

Bitcoin Wiki. (2018, may 21). *SHA-256*. Retrieved from bitcoinwiki: https://en.bitcoin.it/wiki/SHA-256

Bitcoin Wiki. (2018, april 11). *Timelock*. Retrieved from bitcoinwiki: https://en.bitcoin.it/wiki/Timelock

Bitcoin Wiki. (2018, June 3). *Weaknesses*. Retrieved from bitcoin.it: https://en.bitcoin.it/wiki/Weaknesses

Bitcoin.org. (2015, July 4). *Some Miners generating Invalid Blocs.* Retrieved from Bitcoin.org: https://bitcoin.org/en/alert/2015-07-04-spv-mining

Bitcoin.org. (2018, januari 18). *Bescherm uw privacy*. Retrieved from bitcoin.org: https://bitcoin.org/nl/bescherm-uw-privacy

Bitcoin.org. (2018, May 21). *Bitcoin Core version 0.15.0 released*. Retrieved from bitcoin.org: https://bitcoin.org/en/release/v0.15.0#downgrading-warning

Bitcoin.org. (2018, May 1). *Bitcoin Core version history*. Retrieved from bitcoin.org: https://bitcoin.org/en/version-history

Bitinfocharts. (2018, april 12). *Bitcoin Avg. Transaction Fee historical chart*. Retrieved from bitinfocharts.com: https://bitinfocharts.com/comparison/bitcoin-transactionfees.html

Blackmer, S. W. (2016, May 5). *GDPR: Getting Ready for the New EU General Data Protection Regulation.* Retrieved from InfoLawGroup: https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/

Blockchain.info. (2018, June 5). *Bitcoin Hash rate*. Retrieved from blockchain.info: https://blockchain.info/nl/charts/hash-rate

Blockchain.info. (2018, Januari 18). *Blockchain Size*. Retrieved from Blockchain.info: https://blockchain.info/nl/charts/blocks-size

Blockchain.info. (2018, March 1). *Hashrate Distributie*. Retrieved from Blockchain.info: https://blockchain.info/pools?timespan=4days

blockexplorer.com. (2018, Februari 28). *Block #511313*. Retrieved from Block Explorer: https://blockexplorer.com/block/000000000000000004a635e73b78453db8d1ea3d7ef32d0632fa574adde79cb

Braendgaard, P. (2018, Januari 24). *Different Approaches to Ethereum Identity Standards.* Retrieved from medium.com: https://medium.com/uport/different-approaches-to-ethereum-identity-standards-a09488347c87

Brenig, C., Schwarz, J., & Rückeshäuser, N. (2016). Value of Decentralized Consensus Systems - Evaluation Framework. *Ecis 2016 Proceedings*, 1-19.

Brink, A. (2018, March 9). *Three Dimensional Blockchain Scaling with Cosmos and Tendermint*. Retrieved from Youtube: https://www.youtube.com/watch?v=qFPwxHTIhBI

Buchko, S. (2017, December 5). *What is Cardano? Beginner's guide.* Retrieved from coincentral.com: https://coincentral.com/cardano-beginner-guide/

Buterin, V. (2013, March 12). *Bitcoin Network Shaken by Blockhain Fork.* Retrieved from bitcoinmagazine.com: https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/

Buterin, V. (2014). *Ethereum White Paper.* decentralized: ethereum.org.

Buterin, V. (2015, August 7). *On Public and Private Blockchains.* Retrieved from blog.ethereum.com: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Buterin, V. (2015, December 28). *Understanding Serenity, Part 2: Casper.* Retrieved from blog.ethereum.org: https://blog.ethereum.org/2015/12/28/understanding-serenity-part-2-casper/

Buterin, V. (2016, June 17). *CRITICAL UPDATE Re: DAO Vulnerability.* Retrieved from blog.ethereum.org: https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/

Buterin, V. (2016, July 20). *Hard Fork Completed.* Retrieved from blog.ethereum.org: https://blog.ethereum.org/2016/07/20/hard-fork-completed/

Buterin, V. (2016, November 15). *Merkling in Ethereum.* Retrieved from Ethereum Blog: https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/

Buterin, V. (2016, May 9). *On Settlement Finality*. Retrieved from blog.ethereum.org: https://blog.ethereum.org/2016/05/09/on-settlement-finality/

Buterin, V. (2016, October 31). *Uncle Rate and Transaction Fee Analysis.* Retrieved from blog.ethereum.org: https://blog.ethereum.org/2016/10/31/uncle-rate-transaction-fee-analysis/

Buterin, V. (2017, november 25). *BeyondBlock Taipei.* Retrieved from youtube.com: https://www.youtube.com/watch?v=9RtSod8EXn4&feature=youtu.be&t=11493

Buterin, V. (2017, december 19). *Ethereum Wiki / Problems*. Retrieved from GitHub: https://github.com/ethereum/wiki/wiki/Problems

Buterin, V. (2017, februari 23). *Introduction to Cryptoeconomics.* Retrieved from Ethereum Foundation: https://www.youtube.com/watch?v=pKqdjaH1dRo

Buterin, V. (2018, 4 17). *Ethereum Wiki / Sharding FAQ*. Retrieved from GitHub: https://github.com/ethereum/wiki/wiki/Sharding-FAQ

Buterin, V., & Griffith, V. (2017, November 15). *Casper the Friendly Finality Gadget.* Retrieved from https://arxiv.org/pdf/1710.09437.pdf

Calvin, C. (2017, November 16). *Threats to bitcoin (2) - mining Centralization.* Retrieved from medium.com: https://medium.com/@cloudycalvin/potential-threats-to-bitcoin-1-mining-centralization-1fc1090694e5

Cambridge Business English. (2018, March 22). *Interoperability*. Retrieved from https://dictionary.cambridge.org/dictionary/english/interoperability

Cambridge English Dictionary. (2018, March 21). *Privacy*. Retrieved from https://dictionary.cambridge.org/dictionary/english/privacy

Cardano Docs. (2018, May 23). *Cardano Settlement Layer Documentation*. Retrieved from cardanodocs.com: https://cardanodocs.com/technical/protocols/p2p/

Cardano foundation. (2018, May 22). *Project overview.* Retrieved from cardanofoundation.org: https://cardanofoundation.org/project/

Cardano Reddit. (2018, may 31). *Cardano vs. EOS`*. Retrieved from reddit.com: https://www.reddit.com/r/cardano/comments/77ej8i/cardano_vs_eos/

Cardano.org. (2018, May 31). *Philosophy*. Retrieved from Cardano.org: https://www.cardano.org/en/philosophy/

Cardanodocs. (2018, may 31). *Cardano Settlement Layer Documentation - Bootstrap Era*. Retrieved from cardanodocs.com: https://cardanodocs.com/timeline/bootstrap/

Cardanodocs. (2018, may 29). *cardanodocs.* Retrieved from Cryptocurrency basics: https://cardanodocs.com/introduction/#cryptocurrency-basics

Cardanodocs. (2018, may 23). *Ouroboros Proof of Stake Algorithm*. Retrieved from cardanodocs.com: https://cardanodocs.com/cardano/proof-of-stake/

CardanoDocs. (2018, May 23). *Transactions in cardano SL*. Retrieved from cardanodocs.com: https://cardanodocs.com/cardano/transactions/

Castaldi, C., Fontana, R., & Nuvolari, A. (2009). 'Chariots of fire': the evolution of tank technology, 1915-1945. *Journal of Evolutionary Economics 19.4*, 545-566.

Castillo, M. d. (2017, June 2). *Interoperability Boost: Ripple Sends Blockchain Transaction Across 7 Ledgers.* Retrieved from Coindesk: https://www.coindesk.com/interoperability-boost-ripple-sends-blockchain-transaction-across-7-different-ledgers/

Chesbrough, H. (2003). *Open Innovation: The new imperative for Creating and Profiting from Technology.* Boston: Harvard Businnes school press.

CoinMarketCap. (2018, Januari 17). Retrieved from coinmarketcap.com: https://coinmarketcap.com/

Collet, E. (2018, May 23). *From CryptoKitties to Luxury Assets: Non-fungible Tokens are Evolving.* Retrieved from medium.com: https://medium.com/arianee/from-cryptokitties-to-luxury-assets-non-fungible-tokens-are-evolving-1fb08b26e29a

ConsenSys. (2018, Februari 20). *The Inside Story of the CryptoKitties Congestion Crisis.* Retrieved from medium.com: https://media.consensys.net/the-inside-story-of-the-cryptokitties-congestion-crisis-499b35d119cc

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* Thousand Oaks, California: SAGE.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., . . . Wattenhofer, R. (2016). On scaling decentralized blockchains. *International Conference on Financial Cryptography and Data Security* (pp. 106-125). Berlin, Heidelberg: Springer.

CryptoKitties. (2017). *CryptoKitties: Collectible and Breedable Cats Empowered by Blockchain Technology.* Retrieved from CryptoKitties Whitepaper: https://drive.google.com/file/d/1soo-eAaJHzhw_XhFGMJp3VNcQoM43byS/view

Danova, H. (2015, September 2). *What is Bitcoin Fork?* Retrieved from Bitcoin Dictionary: https://blog.cex.io/bitcoin-dictionary/what-is-bitcoin-fork-14622

DiChristopher, T. (2017, december 26). *No, Bitcoin isn't likely to consume all the world's electricity in 2020.* Retrieved from cnbc.com: https://www.cnbc.com/2017/12/21/no-bitcoin-is-likely-not-going-to-consume-all-the-worlds-energy-in-2020.html

Digiconomist. (2018, June 20). *Bitcoin Energy Consumption Index*. Retrieved from Digiconomist.com: https://digiconomist.net/bitcoin-energy-consumption

Dinh, T. T., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2017). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering*, 1-20.

Dosi, G. (1982). Technological paradigms and technological trajectories. *Research Policy 11*, 147-162.

Duncan, L. (2017, July 16). *Liquid Democracy, Ethereum, and the slow path to revolution.* Retrieved from medium.com: https://medium.com/hive-commons/liquid-democracy-ethereum-and-the-slow-path-to-revolution-9c1d5916e706

Economist. (2015, October 31). *The trust machine.* Retrieved from economist.com: https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

Edwards, I. (2018, March 25th). *Roadmap to Bitcoin Developments.* Retrieved from medium.com: https://medium.com/@ianedws/roadmap-to-bitcoin-developments-f7af59b6d122

Ehrsam, F. (2017, November 27). *Blockchain Governance: Programming Our Future.* Retrieved from Medium.com: https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74

Ethereum Community. (2018, april 24). *Ethereum Improvement Proposals*. Retrieved from eips.ethereum.org: http://eips.ethereum.org/

Ethereum StackExchange. (2017, March 17). *What is the exact "longest chain" rule implemented in the Ethereum "Homestead" protocol?* Retrieved from ethereum.stackexchange.com: https://ethereum.stackexchange.com/questions/13378/what-is-the-exact-longest-chain-rule-implemented-in-the-ethereum-homestead-p

Ethereum Team. (2017, October 12). *Byzantium HF Announcement.* Retrieved from Ethereum blog: https://blog.ethereum.org/2017/10/12/byzantium-hf-announcement/

Ethereum Wiki. (2015, November 18). *DEVp2p Wire Protocol.* Retrieved from GitHub: https://github.com/ethereum/wiki/wiki/%C3%90%CE%9EVp2p-Wire-Protocol

Ethereum Wiki. (2015, March 21). *Ethash Design Rationale.* Retrieved from GitHub: https://github.com/ethereum/wiki/wiki/Ethash-Design-Rationale

Ethereum Wiki. (2017, August 3). *Ethash.* Retrieved from GitHub: https://github.com/ethereum/wiki/wiki/Ethash

Etherscan. (2018, May 7th). *Ethereum Network HashRate Growth Chart.* Retrieved from etherscan.io: https://etherscan.io/chart/hashrate

ethstats.net. (2018, april 23). Retrieved from ethstats.net: https://ethstats.net/

Evans, A. (2017, October 17). *A Crash Course in Mechanism Design for Cryptoeconomic Applications.* Retrieved from Medium: https://medium.com/blockchannel/a-crash-course-in-mechanism-design-for-cryptoeconomic-applications-a9f06ab6a976

eWASM GitHub. (2018, June 6). *ewasm/design*. Retrieved from GitHub: https://github.com/ewasm/design

Eyal, I., & Sirer, E. G. (2014). Majority is not Enough: Bitcoin Mining is Vulnerable. (pp. 436-454). Berlin, Heidelberg: Springer.

Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). Cloud Computing and Grid Computing 360-Degree Compared. *Grid Computing Environments Workshop* (pp. 1-10). Leee: GCE'08.

Francesco, C. (2018, Februari 13). *ECB's Draghi says not his job to regulate Bitcoin*. Retrieved from www.reuters.com: https://www.reuters.com/article/us-crypto-currencies-ecb/ecbs-draghi-says-not-his-job-to-regulate-bitcoin-idUSKCN1FX1PW

Gallouj, F., & Weinstein, O. (1997). Innovation in services. *Research Policy 26*, 537-556.

Genestoux, J. (2018, March 5). *Non Fungible Tokens.* Retrieved from Hackernoon: https://hackernoon.com/non-fungible-tokens-5ba83906b275

Github.com. (2018, May 23). *ÐΞVp2p Wire Protocol*. Retrieved from Github.com: https://github.com/ethereum/wiki/wiki/%C3%90%CE%9EVp2p-Wire-Protocol

Graczyk, M. (2018, Februari 1). *Hashgraph: A Whitepaper Review*. Retrieved from Medium: https://medium.com/opentoken/hashgraph-a-whitepaper-review-f7dfe2b24647

Greenwood, P., Hillard, R., Harper, I., & Williams, P. (2016). *Bitcoin, Blockchain & distributed ledgers: Caught between promise and reality.* Australia: Deloitte.

Gupta, V. (2015, March 3). *The Ethereum launch process.* Retrieved from blog.ethereum.org: https://blog.ethereum.org/2015/03/03/ethereum-launch-process/

Hertig, A. (2017, July 21). *BIP 91 Locks In: What This Means for Bitcoin and Why It's Not Scaled Yet.* Retrieved from coindesk.com: https://www.coindesk.com/bip-91-locks-means-bitcoin-not-scaled-yet/

Hertig, A., & Kuznetsov, M. (2018, April 17). *How Ethereum Works.* Retrieved from coindesk.com: https://www.coindesk.com/information/how-ethereum-works/

Hoskinson, C. (2017, Oktober 26). *IOHK | Cardano whiteboard; overview with Charles Hoskinson.* Retrieved from youtube.com: https://www.youtube.com/watch?v=Ja9D0kpksxw

Huenteler, J., Ossenbrink, J., Schmidt, T. S., & Hoffmann, V. H. (2016). How a product's design hierarchy shapes the evolution of technological knowledge - Evidence from patent-citation networks in wind power. *Research Policy 45*, 1195-1217.

Huls, C. (2015). *A Scenario Planning for Interbank Payments and Decentralized Ledger Platforms.* Twente: University of Twente.

Hyperledger Sawtooth. (2018, March 13). *Introduction to Sawtooth*. Retrieved from Sawtooth: https://sawtooth.hyperledger.org/docs/core/nightly/0-8/introduction.html

Interledger. (2018, march 27). *Interledger*. Retrieved from interledger.org: https://interledger.org/

interledger.org. (2018, June 16). *Interledger Protocol (ILP)*. Retrieved from interledger.org: https://interledger.org/rfcs/0003-interledger-protocol/

Intersoft Consulting. (2018, March 15). *Art. 17 GDPR Right to erasure ('right to be forgotten')*. Retrieved from General Data Protection Regulation (GDPR): https://gdpr-info.eu/art-17-gdpr/

IOHK. (2018, march 20). *About*. Retrieved from IOHK.io: https://iohk.io/about/

IOHK. (2018, Januari 17). *Cardano Hub*. Retrieved from Cardano: https://www.cardanohub.org/en/home/

IOHK. (2018, march 20). *Cardano Philosophy*. Retrieved from cardano.org: https://www.cardano.org/en/philosophy/

IOHK. (2018, march 21). *Cardano Roadmap*. Retrieved from cardanoroadmap.com: https://cardanoroadmap.com/

IOHK. (2018, May 29). *IOHK*. Retrieved from Cardano: https://iohk.io/projects/cardano/

ISO. (2018, Januari 26). *ISO/TC 307*. Retrieved from iso.org: https://www.iso.org/committee/6266604.html

Jayachandran, P. (2017, may 31). *The difference between public and private blockchain.* Retrieved from ibm.com: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Johansen, S. K. (2017). A Comprehensive Literature Review on the Blockchain Technology as an Technological Enabler for Innovation. *Mannheim University, Department of Information Systems*, 1-29.

Karapetsas, L. (2018, March 10). *Lefteris Karapetsas - Raiden and state channels.* Retrieved from Youtube.com: https://www.youtube.com/watch?v=93qOwUSj4PQ&t=751s

Karnjanaprakorn, M. (2017, December 7). *The Beginner's Guide to Ethereum's Roadmap*. Retrieved from Hackernoon.com: https://hackernoon.com/the-beginners-guide-to-ethereum-s-2020-roadmap-2ac5d2dd4881

komodoplatform.com. (2018, June 18). *Komodo Decentralized Exchange*. Retrieved from komodoplatform.com: https://komodoplatform.com/decentralized-exchange/

Konstantopoulos, G. (2018, March 27). *The state of Ethereum Scaling, March 2018*. Retrieved from medium.com: https://medium.com/loom-network/the-state-of-ethereum-scaling-march-2018-74ac08198a36

Kostoff, R. N., & Schaller, R. R. (2001). Science and Technology Roadmaps. *IEEE Transactions on engineering management, vol. 48, no 2*, 132-143.

Kravchenko, P. (2017, November 10). *Consensus Explained*. Retrieved from Medium: https://medium.com/@pavelkravchenko/consensus-explained-396fe8dac263

Lamers, D. (2018). *Possibilities for blockchain in the energy transition.* Twente: University of Twente.

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3,*, 382-401.

Larimer, D. (2018, May 29). *Steemit*. Retrieved from Peer Review of Cardano's Ouroboros: https://steemit.com/cardamon/@dan/peer-review-of-cardano-s-ouroboros

LeMahieu, C. (2018). RaiBlocks: A Feeless Distributed Cryptocurrency Network. *Raiblocks Whitepaper*, 1-8.

Lightning Network. (2018, March 27). *Lightning.network*. Retrieved from Scalable, instant Bitcoin/Blockchain Transactions: https://lightning.network/

Lombrozo, E. (2017, Jun 18). *Forks, Signaling, and Activation.* Retrieved from Medium: https://medium.com/@elombrozo/forks-signaling-and-activation-d60b6abda49a

Lundkvist, C. (2017, March 27). *Introduction to zk-SNARKs with examples.* Retrieved from media.consensys.net: https://media.consensys.net/introduction-to-zksnarks-with-examples-3283b554fc3b

Martindale, J. (2017, December 19). *Go ahead, pass laws. They can't kill bitcoin, even if they try.* Retrieved from digitaltrends.com: https://www.digitaltrends.com/computing/dont-worry-about-bitcoin-regulation-it-cant-be-stopped/

Microsoft Docs. (2015, July 20). *Functional Programming vs. Imperative Programming (C#).* Retrieved from docs.microsoft.com: https://docs.microsoft.com/en-us/dotnet/csharp/programming-guide/concepts/linq/functional-programming-vs-imperative-programming

MIT Technology Review. (2017, August 23). *Bitcoin Transactions Aren't as Anonymous as Everyone Hoped.* Retrieved from technologyreview.com: https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/

Morisse, M. (2015). Cryptocurrencies and Bitcoin: Charting the Research Landscape. *Twenty-first Americas Conference on Information Systems* (pp. 1-16). Puerto Rico: University of Hamburg.

Murray, D. (2018, Januari 1). *Ethereum Launches Casper Testnet, Paving the Way for Proof-of-Stake.* Retrieved from blockexplorer.com: https://blockexplorer.com/news/ethereum-launches-casper-testnet-paving-way-proof-stake/

MyungSan, J. (2018). Blockchain government - a next form of infrastructure for the twenty-first century. *Journal of Open Innovation: Technology, Market, and Complexity*, 1-12.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *www.bitcoin.org*, 1-9.

Nelson, R. R., & Nelson, K. (2002). Technology, institutions, and innovation systems. *Research Policy vol. 31, issue 2*, 265-272.

O'Leary, R. R. (2018, Januari 26th). *Part one of Ethereum's Sharding Roadmap is Nearly don.* Retrieved from coindesk.com: https://www.coindesk.com/vitalik-first-part-ethereums-sharding-roadmap-nearly-done/

Oxford English Dictionary. (2018, March 17). *Functionality*. Retrieved from en.oxforddictionaries.com: https://en.oxforddictionaries.com/definition/functionality

Panetta, K. (2017, August 15). *Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017.* Retrieved from Gartner.com: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

Pfeffer, J. (2017, November 24). *ConsenSys / EthOn - An Ethereum Ontology*. Retrieved from GitHub: https://github.com/ConsenSys/EthOn

Phaal, R., Farrukh, C. J., & Probert, D. R. (2004). Technology roadmapping - A planning framework for evolution and revolution. *Technological Forecasting & Social Change 71*, 5-26.

Poon, J., & Dryja, T. (2016). *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.*

Popov, S. (2017). The Tangle. *IOTA Whitepaper*, 1-28.

Ray, S. (2017, December 15). *Hackernoon.com.* Retrieved from Merkle Trees: https://hackernoon.com/merkle-trees-181cb4bc30b4

readthedocs.io. (2018, march 21). *Introduction to Tendermint*. Retrieved from tendermint.readthedocs.io: https://tendermint.readthedocs.io/en/master/introduction.html#what-is-tendermint

Reddit. (2018). *Transactions per second Casper*. Retrieved from r/ethereum: https://www.reddit.com/r/ethereum/comments/7o0a08/transaction_per_second_casper/

Reitwiessner, C. (2016, december 5). *zkSnarks in a nutshell.* Retrieved from blog.ethereum.org: https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/

Reuver, M. d., Bouwman, H., & Haaker, T. (2013). Business model roadmapping: A Practical approach to come from an existing to a desired business model. *International Journal of Innovation Management vol. 17, No. 1* , 1-18.

Rosic, A. (2017, December). *What is Ethereum Casper Protocol? Crash Course.* Retrieved from blockgeeks.com: https://blockgeeks.com/guides/ethereum-casper/

Rosic, A. (2018, May 31). *What is Cardano Blockchain? Step-by-Step Guide.* Retrieved from Blockgeeks.com: https://blockgeeks.com/guides/what-is-cardano/

RSK. (2018, June 20). *About RSK*. Retrieved from rsk.co: https://www.rsk.co/

Saviotti, P. P., & Metcalfe, J. S. (1984). A Theoretical approach to the construction of technological output indicators. *Research Policy 13*, 141-151.

Schiener, D. (2015, November 23). *Liquid Democracy: True Democracy for the 21st Century*. Retrieved from medium.com: https://medium.com/organizer-sandbox/liquid-democracy-true-democracy-for-the-21st-century-7c66f5e53b6f

Schoedon, A. (2018, june 5). *The Ethereum-blockchain size has exceeded 1TB, and yes, it's an issue*. Retrieved from hackernoon.com: https://hackernoon.com/the-ethereum-blockchain-size-has-exceeded-1tb-and-yes-its-an-issue-2b650b5f4f62

Shevlin, R. (2014, December 19). *A Lesson In Mobile Banking Economics*. Retrieved from The Financial Brand: https://thefinancialbrand.com/47336/a-lesson-in-mobile-banking-economics/

Sit, S.-S. (2018, March 13). *Mindset is biggest barrier to blockchain.* Retrieved from Cips.org: https://www.cips.org/supply-management/news/2018/march/invest-in-blockchain-or-risk-falling-behind-ceos-warned/

Sitepu, C. (2017). *A Blockchain-Based Platform Ecosystem Bleuprint for International Trade.* Utrecht: Rotterdam Erasmus University.

Smith, M. J. (1997). Application-specif integrated circuits. *Reading, MA: Addison-Wesley*.

Spenkenlink, H. (2014). *The adoption process of cryptocurrencies.* Twente: University of Twente.

Spode, E. (2017, Februari 14). *The great cryptocurrency heist.* Retrieved from aeon.co: https://aeon.co/essays/trust-the-inside-story-of-the-rise-and-fall-of-ethereum

Store of Value. (2018, Januari 29). *A deep dive into Cardano.* Retrieved from storeofvalueblog.com: http://storeofvalueblog.com/posts/a-deep-dive-into-cardano/

Swan, M. (2015). *Blockchain, Blueprint for a new economy.* Sebastopol: O'Reilly Media, Inc.

Tapscott, D., & Tapscott, A. (2017). *Realizing the Potentail of Blockchain.* Geneva: World Economic Forum.

Techopedia. (2018, march 21). *Bootstrap.* Retrieved from techopedia.com: https://www.techopedia.com/definition/3328/bootstrap

Techopedia. (2018, March 26). *Definition - What does State mean?* Retrieved from Techopedia: https://www.techopedia.com/definition/696/state-computer-science

van Deventer, O. M., Brewster, C., & Everts, M. (2017). *Governance and Busines models of blockchain technologies and networks.* TNO.

Vermeulen, J. (2017, April 22). *mybroadband.co.za.* Retrieved from Bitcoin and Ethereum vs Visa and PayPal - Transactions per second: https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html

Vukoliç, M. (2015). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. *International Workshop on Open Problems in Network Security* (pp. 112-125). Cham: Springer.

Walport, M. (2016). *Distributed Ledger Technology: beyond blockchain.* UK: UK Government Office for Science.

Wang, H., Chen, K., & Xu, D. (2016). A maturity model for blockchain adoption. *Financial Innovation 2:12*, 1-5.

Wang, K. (2017, July 21). *Cryptoeconomics: Paving the Future of Blockchain Technology.* Retrieved from hackernoon.com: https://hackernoon.com/cryptoeconomics-paving-the-future-of-blockchain-technology-13b04dab971

Whycardano.com. (2018, may 23). *Motivation.* Retrieved from whycardano.com: https://whycardano.com/

whycardano.com. (2018, May 29). *whycardano.com.* Retrieved from Why we are building Cardano: https://whycardano.com/science-and-engineering/#why-haskell

Wood, G. (2014). *Ethereum: A secure decentralized generalised transcation ledger.* Etgereum Project Yellow Paper.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview.* U.S. Department of Commerce: National Institute of Standards and Technology.

Yin, R. K. (1984). *Case Study Research; Design and Methods - second edition.* London: SAGE Publications.

Young, J. (2017, December 11). *CryptoKitties Sales Hit $12 Million, Could be Ethereum's Killer App After All.* Retrieved from Cointelegraph.com: https://cointelegraph.com/news/cryptokitties-sales-hit-12-million-could-be-ethereums-killer-app-after-all

Zamfir, V. (2017, december 1). *Against on-chain governance.* Retrieved from Medium.com: https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca

Zamfir, V. (2018, Januari 4). *VladZamfir*. Retrieved from Twitter: https://twitter.com/VladZamfir/status/948908820675297280

Zheng, Z., Xie, S., & Dai, H.-N. (2017). An overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE 6th International Congress on Big Data*, 557-564.

8 Appendix

Appendix I PoET, SBFT, PoA and high level consensus mechanism overview

Proof of Elapsed Time (PoET)

Intel has introduced an additional version of reaching consensus within a network of nodes. Instead of solving heavy computation puzzles like in PoW, each validator is given a random waiting time. This waiting time is 'randomly' generated by a trusted function, also called an enclave, within the Intel processors (Hyperledger Sawtooth, 2018). The processor with the lowest generated waiting time is allowed to generate the block. The probability of being elected as block builder is proportional to the number of processors a single user has to generate waiting times in a trusted enclave (Hyperledger Sawtooth, 2018). A criticism is that the users completely rely on Intel and their secured random generator. If the random generator can be influenced in some way, the way of reaching consensus can be influenced.

Simplified Byzantine Fault Tolerance (SBFT)

There are multiple forms of Byzantine Fault Tolerance based consensus mechanism. Generally, BFT based consensus mechanism work in small networks where validators know each other (Vukoliç, 2015). The ledger thus will become a permissioned ledger. One format of a byzantine fault tolerance protocol is SBFT. The basic idea is that a single validator forms a new block in the chain, and the rest of the validators will validate that block. Consensus about the block will be achieved if a number of validators that is defined by the BFT threshold mark the block as valid (Aumasson & Jovanovic, 2016).

Proof of Authority (PoA)

PoA is a method of reaching consensus that can be used in permissioned ledgers where a single or multiple node(s) are authorized to create new the blocks. In this method of reaching consensus it is assumed that only trusted nodes are authorized as authority. PoA is also mentioned as Proof of Identity in literature (Baars, 2016).

High-level consensus mechanism comparison

Multiple comparisons can be found in literature describing the different characteristics of consensus mechanism (Vukoliç, 2015; Baars, 2016; Kravchenko, 2017; Aumasson & Jovanovic, 2016). Most of them argue about the trade-offs that are in place by comparing different methods of reaching consensus. Table 8.1 shows a comparison derived from Vukoliç (2015) describing the two most contrasted methods of reaching consensus, i.e. PoW and BFT consensus between a group of users. PoS based consensus fits somewhere in between the two (Baars, 2016). PoA will be more efficient than a BFT method of consenus, however a complete trust in the authority is required.

	PoW consensus	BFT consensus
Node identity management	**open, entirely decentralized**	permissioned, nodes need to know IDs of all other nodes
Consensus finality	no	**yes**
Scalability (no. of nodes)	**excellent (thousands of nodes)**	limited, not well explored (tested only up to $n \leq 20$ nodes)
Scalability (no. of clients)	**excellent (thousands of clients)**	**excellent (thousands of clients)**
Performance (throughput)	limited (due to possible of chain forks)	**excellent (tens of thousands tx/sec)**
Performance (latency)	high latency (due to multi-block confirmations)	**excellent (matches network latency)**
Power consumption	very poor (PoW wastes energy)	**good**
Tolerated power of an adversary	$\leq 25\%$ computing power	$\leq 33\%$ voting power
Network synchrony assumptions	physical clock timestamps (e.g., for block validity)	**none for consensus safety** (synchrony needed for liveness)
Correctness proofs	no	**yes**

Table 8.1 **High-level consensus model comparison. Adapted from Vukoliç (2015).**

Appendix II Alternatives to blockchain technologies

Besides blockchain technology, Directed Acyclic Graph (DAG) technology can also be classified as DLT. Although this concept is out scope of this research, for the sake of completeness this subchapter generally explains Directed Acyclic Graph technology. Several DLT solutions that are using DAG technology are IOTA, Hashgraph and Raiblocks (Popov, 2017; Graczyk, 2018; LeMahieu, 2018). The most mature DAG technology currently is used in IOTA and is called the Tangle (Lamers, 2018). One interesting feature of IOTA is that it does not require transaction fees, since each user that sends a transaction into the network has to validate two earlier transaction. Unlike a blockchain, that is a chain of blocks, a DAG is a finite directed graph without cycles without blocks. Figure 8.1 shows an overview of a DAG graph where each block contains a single transaction that has validated two earlier transactions.

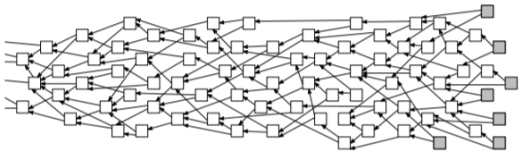


Figure 8.1 **A DAG plot that visualizes the working of IOTA. Adapted from Popov (2017)**

Appendix III Defining the value of a blockchain technology

Although each blockchain technology shares some of the fundamentals, they are not all equal. Therefore, the value created by a single blockchain should be assessed independently. Brenig et al. (2016) designed a framework how to evaluate *decentralized consensus systems* (DCS), in which they also emphasise blockchain technologies. Figure 8.2 shows the value evaluation framework for DCS. In order to evaluate a blockchain. Brenig et al. (2016) distinguish two governance types; open systems and closed Systems. Both types build upon the open and closed innovation paradigms described by Chesbrough (2003). Open innovation is defined as “a paradigm that assumes that firms can and should use external ideas as well as internal ideas, and internal and external paths to market, as the firms look to advance their technology” (Chesbrough, 2003). “Open strategy addresses the challenge of aligning organizations’ business strategy with the openness as a means of expanding value creation” (Brenig, Schwarz, & Rückeshäuser, 2016, p. 7). Examples of open systems communities are the Bitcoin and Ethereum foundations, where the source code of both solutions is open and public and in which the communities pursue an open strategy and promote the development of external applications on their platform. Closed systems are blockchains of private parties where the business model is designed around ownership and control. The source code of these solutions is not open source, and external applications are prevented

from using the blockchain and source code. Importantly, the two type's open and closed systems cannot be distinguished by the organisation profit type. Ripple and Ethereum can both be considered as open system; however, the organisations behind these systems are non-profit in the case of Ethereum and for-profit in the case of Ripple (Brenig, Schwarz, & Rückeshäuser, 2016).

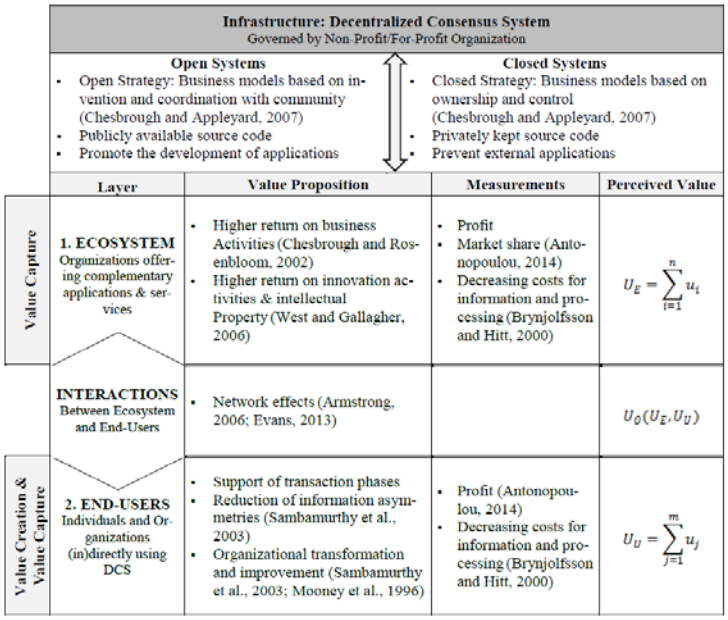


Figure 8.2 **Value evaluation framework for DCS. Adapted from Brenig et al. (2016)**

Besides the distinction of open and closed DCS, Brenig et al. (2016) describe two layers where value is provided within a DCS. Firstly, the ecosystem layer and secondly the end-user layer and additionally the interactions between the two layers.

Ecosystem layer

The ecosystem layer is the layer where the complementary applications and services are located that run on a blockchain. Within the ecosystem, organisations are able to build applications and services on top of the blockchain. Decentralized applications are complementary to blockchains and can provide extended features and functionalities to a blockchain (Sitepu, 2017). A smart contract is examples of an application that is able to verify the interactions between parties and expanding the features of a blockchain (Brenig, Schwarz, & Rückeshäuser, 2016). A service offered on a blockchain could be for example an exchange to trade crypto currencies or a standard crypto payment solution easy to implement for online-shops. Services are not complementary to a blockchain and do not expand the features of a blockchain.

End-user layer

The end-users create value by using the blockchains directly or by using applications that run on a blockchain. End-users benefit from the direct interactions with blockchains due to the reduction of information asymmetry. Additionally End-users can profit from a higher level of transparency and lower transactions costs.

Layer interactions

Between the end-user and ecosystem layer, the network effects come at play. In an open system, when more users start using an application on a blockchain, the value retrieved by the users grows with the increasing number of users. Consequently, if more users start using the system, it becomes more attractive for digital organisations to build their decentralized applications or services upon that

blockchain platform and visa-versa. The system will become self-reinforcing due to the networking-effects. In a closed system, the value will also increase if more users start using the platform; however, it is not possible for organisations to start their own applications or services on a closed blockchain system. Therefore, the network effects will become stronger in the case of open blockchain system leading to a higher system value (Brenig, Schwarz, & Rückeshäuser, 2016).

Appendix IV Blockchain as social technology

MyungSan (2018) introduced an idea of linking the concepts of 'social technology' and blockchain together to create a better understanding of the features regarding blockchain technology. The concept of social technology comes from Nelson and Nelson (2002). They distinguish two types of technologies: 'Physical technology' and 'Social technology'. A physical technology works by a set of rules or standard procedures, i.e. the steam engine, microchips, or a technique of making bronze. When people talk about 'technology', they usually mean a 'physical technology'. A social technology is different and many scholars use the term 'institution' when they refer to a social technology (Nelson & Nelson, 2002). A social technology explains the process of coordination towards a certain outcome. Between people, it could be the process of communication, cooperation, compromise and reaching consensus to reach a certain outcome. However, the two notions of a technology are also interwoven. Physical technology can influence social technology and causes the foundation of a new social technology (MyungSan, 2018). MyungSan (2018) reasons that Nakamoto had used the physical internet technology, to create a new form or an improved version of a social technology. Blockchain technology creates the opportunity to ensure some kind of definitive trust in society. This leads to new forms of communication, cooperation, compromise and reaching consensus between society and within computer systems ensured by blockchain technology. MyungSan (2018) introduces three forms of social trust ensuring technologies that have emerged in history; firstly, the reputation system, secondly the state including government and bureaucracy and thirdly blockchain technology. Except for blockchain technology no systems are available that generate absolute trust based on cryptographic proofs. The reputation systems cannot bring definitive trust since an individual has a maximum number of friends with whom he or she could create and maintain a mutual trust relation. The maximum number of direct friends is able to have and maintain is 150 and is defined by Dunbar's number. The state including government and bureaucracy is a trust system that goes beyond the individual trust system. Myungsan (2018) reasons that the state guarantees trust within a society by introducing bureaucracy including a jurisdiction, security and diplomacy system, although this does not create absolute trust within a system. The third system, blockchain technology is emerging now and is the first social technology system able to create truly person-to-person or peer-to-peer trust relations.

According to the Economist (2015), blockchain technology could transform the way in which economies work. Blockchain technology make it possible for people that does not know or see each other to work together without going to a neutral central authority. A blockchain system enables people to interact without trust concerns, making a transaction "trust free" (Beck, Stenum Czepluch, Lollike, & Malone, 2016). According to Beck et al. (2016), blockchains applications like Decentralized Autonomous Organisations compete with centralized hierarchical organizations like firms and governments. Functionally this would mean that a blockchain as technology would make decentralized institutions possibly leading to new forms of social technology.

Appendix V Interview Guide – Blockchain Technology

Interview info:	Place information: Date: Recorded:
Introduction:	Thank note towards Interviewee. Introduction research and public blockchain viewpoint. The purpose of the interview. Ask for unclearness
Interviewee info:	Name: Company info: Function:
What is your opinion on public versus private blockchain technologies?	
What are the key challenges of current public blockchain technologies?	
How do you think blockchain technologies could scale?	.
What is your opinion about Payment channels, sharding, Plasma etc.?	
How will blockchain protocols solve privacy issues into the future?	
Since Ethereum is testing Casper, What is the benefit of PoS in comparison to PoW?	
What is your opinion about Cardano?	
What do you think is the most trustworthy blockchain platform currently?	
Validation:	Explain the current conceptual model, and ask interviewees there opinion.
Thank you Note	

Interview Guide – Blockchain Use cases

Interview info:	Place information: Date: Recorded:
Introduction:	Thanks note towards Interviewee. Introduction of the research and the public blockchain point of view. The purpose of the interview. Ask for unclearness
Interviewee info:	Name: Company info: Function:
How do you define a blockchain technology?	
Why do you have high interested in public blockchain technologies?	
Can you give a short description about the current use case you are working on?	
On what blockchain platform are you currently working?	
What is the reason that you picked this platform?	
What are the mayor challenges in the implementation of your use case?	
How do you work together with other stakeholders in the solution?	
Validation:	Explain the current conceptual model, and ask interviewees there opinion.
Thank you Note	

Appendix VI Cardano Philosophy list. Derived from Cardano.org (2018)

- Separation of accounting and computation into different layers
- Implementation of core components in highly modular functional code
- Small groups of academics and developers competing with peer reviewed research
- Heavy use of interdisciplinary teams including early use of InfoSec experts
- Fast iteration between white papers, implementation and new research required to correct issues discovered during review
- Building in the ability to upgrade post-deployed systems without destroying the network
- Development of a decentralized funding mechanism for future work
- A long-term view on improving the design of cryptocurrencies so they can work on mobile devices with a reasonable and secure user experience
- Bringing stakeholders closer to the operations and maintenance of their cryptocurrency
- Acknowledging the need to account for multiple assets in the same ledger
- Abstracting transactions to include optional metadata in order to better conform to the needs of legacy systems
- Learning from the nearly 1,000 altcoins by embracing features that make sense
- Adopt a standards-driven process inspired by the Internet Engineering Task Force using a dedicated foundation to lock down the final protocol design
- Explore the social elements of commerce
- Find a healthy middle ground for regulators to interact with commerce without compromising some core principles inherited from Bitcoin

Appendix VII Mayor differences between Imperative and functional programming. Derived from Microsoft Docs (2015)

CHARACTERISTIC	IMPERATIVE PROGRAMMING	FUNCTIONAL PROGRAMMING
PROGRAMMER FOCUS	How to perform tasks (algorithms) and how to track changes in state.	What information is desired and what transformations are required.
STATE CHANGES	Important.	non-existent
ORDER OF EXECUTION	Important.	Low importance.
PRIMARY FLOW CONTROL	Loops, conditionals and function (method) calls.	Function calls, including recursion.
PRIMARY MANIPULATION UNIT	Instances of structures or classes.	Functions as first-class objects and data collections.