The Advantages and Challenges of the Blockchain for Smart Grids

T.M.G.L. Winter

TU Delft

The Advantages and Challenges of the Blockchain for Smart Grids

by

T.M.G.L. Winter

to obtain the degree of Master of Science
at the Delft University of Technology,
to be defended publicly on Wednesday May 30, 2018 at 14:00 PM.

Student number:	4111435	
Project duration:	June 1, 2017 – May 30, 2018	
Thesis committee:	Prof. dr. ir. P. Bauer,	TU Delft, supervisor
	Dr. S. H. Tindemans,	TU Delft
	Dr. ir. L. M. Ramirez Elizondo	TU Delft
	Ir. N. van der Blij,	TU Delft, supervisor

This thesis is confidential and cannot be made public until May 30, 2018.

TU Delft

Preface

During the past 9 months researched have been performed on the application of the Blockchain in assignment of the Electrical Sustainable Energy department of the Technical University of Delft. This thesis is written as part of the final assessment of the master sustainable energy technology.

The main goal of the research is to identify the opportunities, advantages and technical challenges of applying the Blockchain to the electrical power system. The research has been performed in a time period of 9 months.

First, research has been performed on the Blockchain in order to define the Blockchain and study the working principles behind the Blockchain. Second, the current Dutch electrical power system has been studied and opportunities where the Blockchain could be applied in the electrical power system have been identified. This has resulted in four case studies which have been used throughout the thesis. Third, the advantages of applying the Blockchain to the electrical power system have been explored based on the different case studies. Fourth, the technical challenges of applying the Blockchain to the electrical power system have been identified and potential solutions to some of the challenges have been discussed. Fifth, the actual application of the Blockchain to the electrical power system based on the different case studies has been discussed.

During the process of performing the research and writing the thesis I have learned a lot from the people who have assisted me. Especially I would like to thank ir. Nils van der Blij, ir. Pavel Purgat and Prof. dr. ir. Pavol Bauer for their help and guidance during the process.

Abstract

In our current society both the demand for electricity is increasing and the demand for electrical energy as energy carrier is increasing. Renewable sources will play an important role in future energy generation due to societal developments. These distributed energy resources introduce new challenges to our current electrical power system. One of these challenges imposed on our current electrical power system is the introduction of a new grid user, the prosumer, who consumes and produces electrical energy. Another challenge is the intermittent nature of renewable sources such as solar and wind energy.

During the past year Blockchain gained momentum as a technology mainly through the evolving industry of cryptocurrencies such as Bitcoin and Ether. Application of the Blockchain to the electrical power system could offer solutions to some of these challenges that the future electrical power system will face. The main goal of this thesis is to identify the opportunities, advantages and technical challenges of applying the Blockchain to the electrical power system.

First, as part of the literature study the Blockchain has been studied and the operation of the Blockchain has been analyzed. The Blockchain has been defined as a collective of technologies that can be described as a database, which is distributed among a peer to peer network, combined with securitization elements relying on multiple cryptographic technologies.

Second, the opportunities where the Blockchain could be applied in the current electrical power system were identified. In order to study the application of the Blockchain to the electrical power system four case studies have been introduced. These case studies differentiate themselves in the level of adoption of the Blockchain and the functionality which could be provided to the electrical power system. Ranging from a local peer to peer trading infrastructure to the entire market being operated via the Blockchain with advanced features such as the control of power flows.

Third, the various advantages of applying the Blockchain to the electrical power system have been explored based on the proposed case studies. A distinction has been made between advantages which are inherently linked to the characteristics of the Blockchain and the provided functionality to the electrical power system.

Fourth, the challenges of applying the Blockchain to the electrical power system have been analyzed and discussed. Based on the different case studies a segregation has been made between challenges attributable to the characteristics of the Blockchain and challenges specifically linked to the implementation of the case studies.

Last, the practical application of the Blockchain to the electrical power system of the different case studies have been discussed. Explanation is given how the different case studies could be implemented within the electrical power system and what the role will be of different parties currently involved within the electrical power system.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter discusses the background of the thesis. In section 1.1 the motivation of researching the application of the Blockchain for smart grids is explained. In section 1.2 the scope and goals of the thesis are explained. In section 1.3 the layout of the thesis is discussed.

1.1 Motivation

In today's society energy demand is ever increasing and the demand for electricity as energy carrier is increasing even faster. Due to societal and technical developments it will be inevitable that power generation from renewable energy sources will play a more important role in order to fulfill the energy demand. Of all renewable energy sources, solar and wind energy will contribute for a large share in current and future generation. Compared to traditional power generation these distributed energy sources have specific characteristics which introduce new challenges to the current distribution system.

One of these challenges is the introduction of a new type of grid user called the prosumer, who consumes and produces energy in a local fashion. Another challenge is the intermittent nature of renewable energy sources such as solar and wind energy.

The principal task of the electricity grid is to transmit energy in a stable manner. Smart grids propose a solution to the integration of these distributed energy sources in order to maintain security of supply of the electricity grid. The focus of smart grids is to facilitate local production and consumption by prosumers and consumers.

By stimulating local energy production and consumption transmission losses are reduced. Prosumers and consumers should be able to trade electricity with each other in a peer to peer fashion. To manage these transactions between consumers and prosumers participating within the smart grid in a centralized manner would likely to be very costly and would require complex communication infrastructure. As a result it would be clear that a decentralized method would be preferred.

Applications based on Blockchain could offer solutions to problems of different levels of complexity within the smart grid. At first as a primary introduction, the application of Blockchain could offer a solution in order to establish a trading infrastructure within the smart grid. Ideally the application of the Blockchain would enable parties, in this case consumers and prosumers within the smart grid, to trade electricity with each other in a peer to peer fashion without the intervention of a third party to ensure trust.

The application of a Blockchain based trading infrastructure within the smart grid promises a range of benefits. For example, one could think of advantages such as: the establishment of a real time market, less transaction cost due to a simplified trading structure and more privacy for users within the smart grid.

Besides utilizing the Blockchain for realizing a trading infrastructure more sophisticated and complex applications could be established by adding computational functionality. As a result a decentralized computing platform can be created which could be used to offer a variety of solutions within smart grids.

For example, control within the smart grid could be enforced by variable pricing. Consumers and prosumers are economically incentivized to produce or consume energy based on real time market pricing dependent on the availability of energy resources.

1.2 Thesis scope and goals

In section 1.1 the motivation of researching the application of the Blockchain for smart grids was explained. In order to gain a full understanding of the application of the Blockchain for smart grids it is important to define a clear scope and goals of the thesis. The scope of this thesis is narrowed down to performing research on the Blockchain and its application for smart grids rather than actual implementation.

Extensive research will be performed on different technologies behind the Blockchain in order to gain full understanding of its potential application. The areas of the grid where the Blockchain could be applied will be identified and analyzed. The advantages and technical challenges of the implementation of the Blockchain for smart grids will be explored in great detail. This research will be performed on the basis of case studies.

The main goal of this thesis is to identify the opportunities, advantages and technical challenges of applying the Blockchain to smart grids.

The main goal can be split up into four parts.

- What is the Blockchain and how does it operate ?
- Where in the smart grid can the Blockchain be applied ?
- What are the advantages of these applications of the Blockchain to smart grids ?
- What are the (technical) challenges for applying a Blockchain for smart grids ?

Firstly, a full understanding of the Blockchain is obtained. The different technologies of the Blockchain will be studied. An overview of the modus operandi of the Blockchain will be provided. As a result the reader should have a clear overview of Blockchain and the technologies behind it after reading this thesis. It should give the reader insight in the following topics such as distributed ledger technology, the applied cryptographic securitization, mining protocol, the consensus mechanism.

Secondly, the goal is to identify the advantages of applying a Blockchain for smart grids. In order to identify the advantages it is important to study the current grid structure and define areas of application where the Blockchain could be applied. After identification of the areas of application extensive research will be performed on the advantages of implementation of the Blockchain compared to the current grid structure.

Thirdly, This goal should expose the different technical challenges of the application of the Blockchain for smart grids. The question will focus on the technical challenges which are faced during implementation of a Blockchain for smart grids rather than social challenges to overcome.

1.3 Layout of the thesis

The previous sections covered the motivation and the scope and goals of the thesis. This section will highlight the content per chapter.

Chapter 2

Chapter 2 will explain to the reader what a Blockchain is and will analyze the operation of the Blockchain. The history of the Blockchhain will be provided to the reader. An overview will be presented and the multiple technologies involved in the Blockchain will be explained to the reader.

Chapter 3

In chapter 3 the opportunities for applying the Blockchain to the existing electrical power system have been identified. In the beginning of the chapter several aspects about the existing electrical power system have been explained and an overview has been presented of the parties involved. After identification of the potential areas for applying the Blockchain four case studies have been introduced which are used throughout the thesis.

Chapter 4

In chapter 4 the various advantages of applying the Blockchain to the electrical power system have been analyzed and discussed based on the case studies. A distinction has been made in advantages which are attributable to the characteristics of the Blockchain and the provided functionality to the electrical power system.

Chapter 5

In chapter 5 the challenges of applying the Blockchain to the electrical power system have been analyzed and discussed. At the beginning of the chapter the challenges inherently linked to the characteristics of the Blockchain have been discussed. Throughout the continuation of the chapter the challenges to the electrical power system and the challenges specifically linked to the implementation of the case studies are exposed and discussed.

Chapter 6

In chapter 6 the practical application of the Blockchain to the electrical power system of the different case studies has been discussed. An explanation is given how the case studies could be implemented and what the role will be for the parties involved in the existing electrical power system.

Chapter 7

In chapter 7 the results of the thesis have been outlined and a interpretation of the results has been provided to the reader in the discussion.

Chapter 2

What is a Blockchain

This chapter will explain to the reader what a Blockchain is. Section 2.1 will give the reader insight the history of the Blockchain. Section 2.2 will provide an overview of the Blockchain. In section 2.3 the network architecture will be explained to the reader. Section 2.4 and section 2.5 will provide insight about cryptography and it's application for the Blockchain. Section 2.6 will explain to the reader how mining and the consensus mechanism work.

2.1 A brief history of the Blockchain

The first application based on a Blockchain was conceptualized and implemented by the anonymous alias Satoshi Nakomoto in 2008. In his research paper, Bitcoin: a peer to peer electronic cash system, he described how a electronic peer to peer currency could be established without the requirement of any intermediary institutions e.g. financial institutions such as banks, regulating authorities such as central banks, etc [1].

The theoretical framework of the first decentralized digital currency was established and the currency was called Bitcoin. In the first instance there was a lot of skepticism and criticism from the cryptographer community about the described concept. Whether it would be possible to establish a truly digital and decentralized currency because leading computer scientists have been trying to create such a system for long time and failed. Previous attempts such as Digicash and Ecash could be considered as the predecessors of Bitcoin [2].

In the following year the first version of Bitcoin was implemented and released as an open source software project by the same alias Satoshi Nakomoto. After the release and implementation of the software the first monetary transaction within the Bitcoin environment took place on the 12th of January between Satoshi and Hall Finney, which was one of the early adopters of Bitcoin. The transaction, which was conducted as a test, consisted out of a transfer of 10 Bitcoins from Satoshi to Finney which would have a value of 40.000 Us dollars by today [2].

After the launch of Bitcoin an online community of developers arose which aimed on the further development of the software. Satoshi Nakomoto participated within this community revising the software until 2011. Afterwards there has not been any public / online interaction and until today his identity still remains unknown. However, there have been multiple claims about the knowledge of his identity. Over the past years the community formalized by forming institutions such as the Bitcoin foundation, which aims to educate people about the various aspects of bitcoin and accelerate the use of it [2, 3].

During the past decade since the launch Bitcoin gained popularity and momentum as a currency. However, people were skeptical at first whether it would be possible to establish a truly decentralized payment method and currency in a secure fashion. However, as time past they observed the reliability of the system and the absence of security breaches. Which lead to increasing interest in the working technologies behind Bitcoin [2, 3].

From different viewpoints one can conclude that Bitcoin is gaining acceptance within today's society. From a social perspective it is gaining acceptance, where the currency was first linked to criminal activities such as money laundering of illegal activities and as a payment method of the infamous online drug trading platform called the silk road. More users with legal intentions are engaging in making payments via Bitcoin and more companies are accepting Bitcoin and other cryptocurrencies as a official payment method.

Recently the market capitalization of the bitcoin reached over 50 billion US dollars and it reached a twenty four hour trading volume of 130 million US dollars . From legal perspective the majority of governments in the western world such as the countries in the European union and US have acknowledged the legality of bitcoin as a currency [2, 4, 5].

From academic perspective there is an increasing interest in Bitcoin and more research is devoted on the working technologies behind it. As mentioned before it was the first truly decentralized digital currency which allowed users of the system to trade and make transactions with each other in a peer to peer fashion without the requirement of third parties to enforce trust.

The success of Bitcoin relies to a great extent on the collective of technologies referred to as the Blockchain. The Blockchain can be described as a database with securitization elements relying on multiple cryptographic technologies distributed across a peer to peer network. The majority of these technologies were already invented before Satoshi Nakomoto combined these as an collective, which lead to the invention of the Blockchain [1].

Since the invention of the Blockchain people started to explore the possibilities of creating different applications based on the Blockchain, which lead to multiple successful Blockchain based applications such as for example the first decentralized computing platform called Ethereum [3,6].

2.2 An overview of the Blockchain

In this subsection the reader will be given an overview of the Blockchain in order to get a basic understanding before diving into technical details. The Blockchain is a collective of technologies and can be described as a database, which is distributed among a peer to peer network, combined with the securitization elements relying on multiple cryptographic technologies. The Blockchain consists out of a collective of technologies. The most important technologies are: distributed ledger technology, cryptographic technologies and the consensus mechanism [1, 3, 7].

The majority of Blockchain based applications are based on a peer to peer network architecture. Typically participants of the application are connected with each other via internet and form a network together. Within this network all participants are referred to as peers because each of them are equally privileged within the network and none of the participants has special rights [1, 7].

In general the Blockchain enables peers, which participate in the underlying network, to store and write transactions securely in a decentralized fashion e.g. without the requirement of trusted third parties. In the majority of Blockchain based applications these transactions resemble the transfer of an asset which contains value, whether this is a currency transaction in the case of Bitcoin, a request to perform computations on the Ethereum platform or a change of ownership to the entitlement of a piece of land.

The records of these transactions are stored on a ledger. One could imagine the ledger as an accounting book, where in bookkeeping all financial transactions of a company are stored. On the ledger of a Blockchain based application the total history of all occurred transactions is stored. A copy of this ledger is distributed and stored among all peers which participate in the underlying network of the Blockchain. Therefore each peer which participates in the network possesses a copy of the ledger containing data of the total transaction history [1, 3, 7].

The applied cryptographic securitization technologies make establishing new transactions and storing those transactions onto the ledger very secure. In general a transaction can be defined as a digitally signed piece of data, which contains information about the transfer of an asset based on the specific Blockchain based application. The applied cryptographic securitization method allows users to create signatures corresponding to a designated transaction in a very secure manner [8].

One could imagine a transaction like a check, the check is only valid if it was signed by the owner of the corresponding bank account. Due to the applied cryptographic securitization it is very hard to alter transactions once they have been signed or to forge a signature.

The combination of the fact that everyone possesses a copy of the ledger and the applied cryptographic securitization makes storage of data onto the ledger very secure. Once transactions have been stored onto the ledger it would be very hard for a malicious attacker to forge or delete these transactions.

Transaction data is stored onto the ledger in small packages. Due to the applied cryptographic securitization transaction data is stored in such manner that links are created between newly stored packages of transaction data and earlier stored packages of transaction data, if one would try to alter or delete data within these packages the links will be broken between the packages. Because everyone possesses a copy of the ledger it will be easily detected when one of those links were broken [1, 7].

One of the key technologies of the Blockchain is the consensus mechanism. The consensus mechanism ensures that each peer which participate in the network agrees on the modifications of the ledger. The consensus mechanism consists out of four elements [3, 9].

Verification of newly created transactions by each peer according to a specific set of rules, for example one of these rules is that a transaction is only considered valid if the correct signature is provided with the transaction [3, 9].

The verified transactions are compiled in small packages called blocks by peers, who engage in a process called mining. The peers who engage in the mining process are called miners. The miners provide a part of their computational power by executing a computational complex problem in exchange for an economic incentive. Only when miners create valid blocks the miners are economically rewarded. This induces an economic incentive to act in a honest manner [10].

The third step consists out of the validation of the newly created blocks by each of the peers participating within the network according to the consensus rules. In the last step consensus is derived about the valid state of the ledger [3, 9].

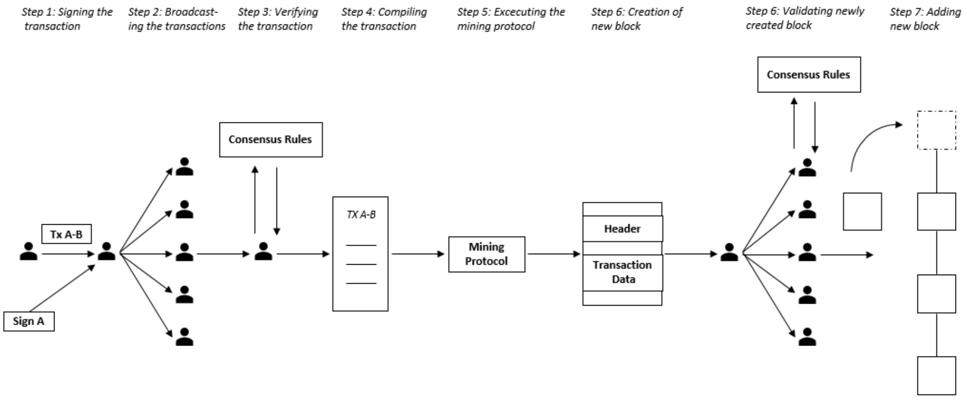


Figure 2.1: Simplistic Overview of the Blockchain

In figure 2.1 one can see a simplistic overview of the described processes of the Blockchain. One could see in the figure that peer A wants to establish a transaction with peer B. In order to establish a valid transaction an important step is to generate a correct signature. The signature is generated with the applied cryptographic securitization method, which is often referred to as public key cryptography.

After creation of the transaction peer A will broadcast the transaction to other peers via the network, this is shown in step 2 of figure 2.1. After receipt of the transaction the other peers will verify the transaction independently according to the consensus rules, when the transaction is considered valid the peer will broadcast the valid transaction to other connected peers. In this way valid transactions propagate quickly through the network until every participating peer in the network has received the newly created transaction.

Afterwards the newly created transaction is compiled by peers, who engage in the mining process. These peers who engage in the mining process are called mining nodes. The mining nodes will compile newly created transactions into blocks often multiple newly created transactions are compiled in a block. The mining nodes will dedicate a part of their computational power in exchange for an economic incentive by executing the mining protocol. The execution of the mining protocol involves finding a solution to a mathematical puzzle which is in general computationally exhaustive. In order to stimulate mining nodes to engage in this process they are economically rewarded.

The required up front devotion of computational power of the mining nodes results in honest behavior because the economic reward of creating a block will be granted retrospectively and only when the transaction included in the block are considered to be valid. This phenomena incentivizes mining nodes to act purely honestly, by only including valid transactions within the block, otherwise they might lose their economic reward afterwards.

After the mining node has found a solution to the mining protocol it will broadcast the new block to the other connected peers. These peers will verify the block independently according to the consensus rules, for example whether it was constructed in the righteous manner and if it only includes valid transactions etc. When the majority of peers agree on the fact that the block is valid it will be recorded to the ledger, this is shown in step 7.

2.3 Networks

In order to get an understanding how the Blockchain works it is essential to have a clear view about the underlying network of Blockchain based applications. There are multiple types of network designs which have a major influence on the properties of the Blockchain.

The most common structure, which is used for Bitcoin and the decentralized computing platform Ethereum, is the peer to peer network structure. Every computer which participates in the network is called a node and is connected with other nodes. In the peer to peer network architecture each node communicates with different connected nodes directly, there is an absence of an hierarchical structure compared to an client server structure for example [3, 6, 7]. This is shown in figure 2.2.

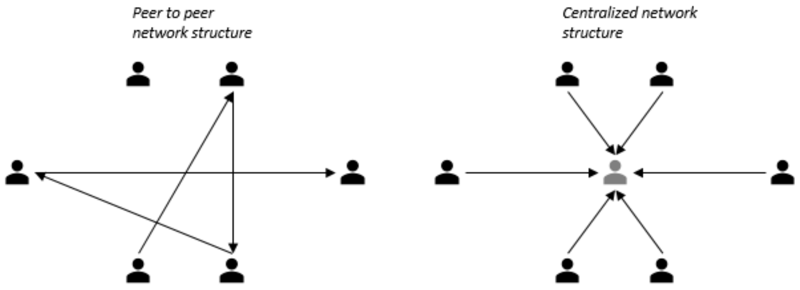


Figure 2.2: Comparison of peer to peer network structure vs centralized network structure

All nodes which participate in the network provide and consume services and are equally privileged hence there is no hierarchy between nodes themselves. However, they can adopt different roles within the network such as full node, mining node, lightweight node or a combination of these [3, 6, 11].

The underlying network structure of Bitcoin and Ethereum is characterized by the classifications public and permissionless. Public is defined as that each node has the ability to receive a full copy of the distributive database and that there are no restrictions on joining the network, private defines the opposite of public where there are restrictions on reading data and joining the network [3, 11].

The classification permission less is defined as that there are no restrictions on nodes which can participate in the consensus process of the Blockchain, permissioned defines the opposite where there is a restriction on nodes which can participate in the consensus process. In the table 2.1 an overview is given of the different classifications [3, 11].

Table 2.1: Overview of different network classifications

	Permissionless	Permissioned
Public	No restrictions on identities in reading data or participating in consensus mechanism.	No restrictions on identities in reading data however participating in consensus mechanism is restricted.
Private	Restrictions on identities in reading data, no restrictions on participating in consensus mechanism.	Both reading data and participating in consensus mechanism are restricted.

2.3.1 Nodes and their roles

Peers who participate within the network are referred to as nodes. These nodes can adopt different roles within the network. In general for Blockchain based applications the following types of nodes can be distinguished: The full node, the lightweight node and the mining node. Each type of node provides specific functionalities based on its role. However, all types of nodes possess the routing functionality of broadcasting transactions to connected peers within the network [3].

2.3.2 Full nodes

Full nodes distinguish themselves from other types of nodes. Full nodes store a entire copy of the distributed ledger which include the total history of all occurred transactions. All blocks which include the total transaction history since the genesis block are stored by the full nodes. Because full nodes possess a full copy of the distributive ledger they have the ability to verify transactions autonomously without the reliance on information from other nodes. Because full nodes possess a full copy of the distributed ledger it uses a lot of data to store a full copy of the ledger. Which might not always be suitable for certain types of devices. Besides verifying transactions full nodes engage in routing functions such as broadcasting new transactions to other interconnected peers [3, 6].

2.3.3 Lightweight nodes

In general it takes a lot of storage to keep a full copy of the distributed ledger of a Blockchain based application. Often this is simply too large for devices such as mobile phones, mobile laptops etc. In order to enable more users to participate in the network a there is the ability to only store a partial copy of the distributive ledger. Light weight nodes only store the headers of the blocks which reduces the required storage greatly. In order to verify a transaction the lightweight node relies on information of full nodes. The lightweight node requests from several full nodes a proof of inclusion of a transaction in the block, if the request of the different nodes correspond with each other the header of the block will be added to the partial copy of the distributive ledger of the lightweight node. Besides simple verification the lightweight nodes broadcast new transactions to other connected nodes [3, 7].

2.3.4 Mining nodes

Mining nodes compete with each other in executing the mining protocol as part of the consensus mechanism of the Blockchain. The mining node devotes his computational power by executing the mining protocol for an economic incentive. The mining node can maintain a full copy of the distributive ledger at the same time hence being a full node at the same time, but it is not necessary. Nowadays running a mining node is more competitive than in the earlier days of the Bitcoin Blockchain therefore the chances of finding the solution to the mining protocol as a miner with modest computational power is very small. Miners collaborate in pools forming one mining node and are rewarded by their devotion of computational power within the pool [3, 6, 11].

2.4 Public key cryptography

Public key cryptography is one of the primary technologies used in Blockchain technology. Public key cryptography was invented in the mid seventies of the previous century by Martin Hellman, Whitfield Diffie and Raphael Merkle [12].

Public key cryptography is based on a key pair which consist out of a public key and a private key. The public-private key pair is used in order to encrypt and decrypt messages. Encryption is the process of "locking" a message, which usually contains a piece of confidential information, in such a way that the content of the original message is concealed. The reverse process is called decryption, where approved parties with authorization can decrypt an encrypted message in order to reveal the original information [12, 13].

The public and private key are mathematically related to each other in how they were constructed. The public key is constructed from the private key via a mathematical algorithm which acts like a trapdoor function. Therefore generating a public key from the private key is computational easy however constructing a private key from a public key is computationally infeasible even if the specific algorithm of constructing the key pair was known. The public key does not contain any confidential information and and can be visible to everyone, opposed to the private key which should be kept secret at all cost [12–14].

In figure 2.3 an illustration is shown how the public key is generated from the private key via a trapdoor function.

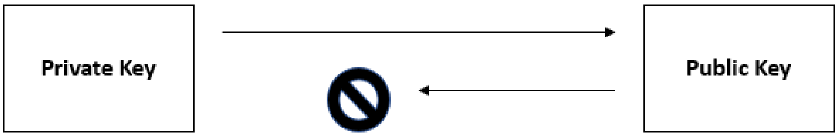


Figure 2.3: Schematic overview trapdoor function

These trapdoor functions are typically based on mathematical problems such as the discrete logarithmic problem or integer factorization problem. Elliptic curve cryptography, which relies on the discrete logarithmic problem, is used by the majority of Blockchain based applications as public-private key generation algorithm and as part of the verification algorithm [14, 15].

Public key cryptography is mainly used for two appliances. Public key encryption, where a message is encrypted and decrypted with the public-private key pair of the recipient. The message is encrypted with the public key of the recipient and in order to decrypt the message the private key of the recipient has to be used. Only the recipient has access to his private key and therefore the recipient is the only party who can decrypt the message in order to gain access to the specific information contained in the message [13, 15].

The other main application of public key cryptography is used for constructing digital signatures. The sender of a message, containing specific information, can construct a digital signature with his private key. This digital signature is dependent on the content of the message and the private key of the sender. The signature can be verified with the public key of the sender. One could consider the digital signature as a seal which ensures authenticity and integrity of the message [13, 15].

The latter appliance of public key cryptography is mainly used by Blockchain based applications. In general ownership of assets recorded onto the distributed ledger of Blockchain based applications is established via public key cryptography.

Typically a transaction is established between two addresses, the address of the payer and the address of the payee. Each address has a key pair linked to it which consist out of a public key and a private key. Funds can considered to be linked to an address via its corresponding public key. Similar to a savings account of a regular bank one could think of the public key as the account number and the address as the corresponding name to the account number [3, 6, 7].

As mentioned before each address is generated from a key pair, which consist out of a public and private key. The private key is used to create a signature for a transaction. The public key is generated via cryptographic securitization from the private key [3].

A transaction is only considered valid if it has the correct signature and these signatures are generated with the private key. The private key enables control over the assets linked to the corresponding address, therefore it establishes ownership over the linked assets to the specific address Andreas.

It is of great importance for the end user to keep his private key to his corresponding address secure and safe. In most cases the key pair is stored in a digital file within the software of the wallet.

2.4.1 Elliptic curve cryptography

The applied public key cryptography of the majority of Blockchain applications is based on elliptic curve cryptography. Neil Koblitz and Victor Miller were the first to introduce the usage of elliptic curves in cryptography in 1985. Since introduction and usage of elliptic curves in cryptography a lot of research has been performed on their security performance and it shows that higher levels of security can be reached compared to conventional securitization methods such as RSA [16].

The working principle behind the applied elliptic curve cryptography is the usage of the discrete logarithmic problem. The use of the discrete logarithmic problem makes it possible to create a trapdoor function which means computing the outcome one way is trivial but if one would want to calculate the input from the outcome than this procedure would be computationally infeasible [8].

The applied elliptic curve cryptography for the majority of Blockchain based applications relies on a set of operations with the elements of a elliptic curve. For a set of points on an elliptic curve two operations can be defined. These operations together with the set of points of the elliptic curve form a group. A group is an abstract mathematical structure where the elements together with the operation have certain mathematical properties [3, 7, 13, 15].

Two operations can be defined together with the elements of the elliptic curve, *point addition* and *point doubling*. In figure 2.4 the geometrically representation of point addition is shown [8,13,15,16].

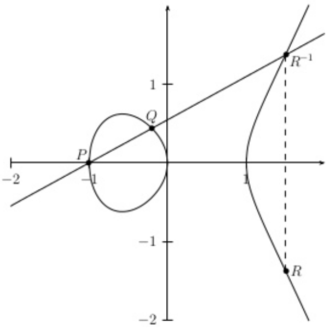


Figure 2.4: Geometrical representation of point addition

P(x1,y1), *Q(x2,y2)*, *R(x3,y3)* are points on the elliptic curve. If a line is drawn through points P and Q on the curve there exists a third point of intersection on the curve R^{-1}. R is the inverse of R^{-1}. The operation is defined as $P + Q = R$ [8,16].

Point doubling is geometrically displayed in figure 2.5.

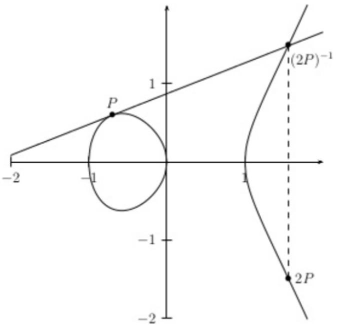


Figure 2.5: Geometrical representation of point doubling

Let *P(x1,y1)* be a point on the elliptic curve. If a line tangent to point P is drawn it will intersect a second point on the elliptic curve $2P^{-1}$. The point 2P is the inverse of $2P^{-1}$. Point doubling is defined as $P + P = 2P$. [8,13,15,16].

Our defined operation point addition makes it possible to define scalar multiplication. Let G be a point on the curve and k an integer. Scalar multiplication can be defined in the following manner $P = k \circ G = (G + G + G + G..k)$ [8].

The elliptic discrete logarithmic problem can be described as finding an integer k when the point P and G on the elliptic curve are known which satisfies the following equation $P = k \circ G$. In order to find a solution to the problem of finding k an addition should be made repeatedly of G, 2G, 3G until the value of k is found. By using large enough values for integer k this problem becomes very hard [8,16].

The crux of the elliptic curve discrete logarithmic problem lies in the fact that the forward calculation is computational easy and the hardness of the inverse calculation. By implementing a algorithm which combines point doubling and addition together it is computational easy to perform the forward calculation [8].

2.4.2 Private keys and public keys

The primary purpose of the applied cryptography for Blockchain based applications is to enable users to create signatures with their private key. The private key enables control over the assets linked to the specific address hence it establishes ownership over these assets.

The public key is constructed out of the private key via elliptic curve scalar multiplication, which is executed by a combination of point doubling and point addition operations [3, 7]. The address is created from the public key by applying a hashing function on the public key. Hashing functions are pseudo-random functions which act like trapdoor function hence computing the inverse is very difficult. Hashing functions are further explained in section. The hashing function is applied in the majority of Blockchain based application in order to create an extra layer of protection to secure the private key against malicious attacks [3, 7].

An overview of the relation between address, public key and private key is shown in figure 2.6.

Figure 2.6: Overview relation address, public key, private key

2.4.3 Private key

In the majority of Blockchain based applications the private key is a 256 bit number. It is important to store the private key securely. The key is usually stored within the software of the wallet. Often private keys are generated by the designated wallet software [3, 7]. The process of generating the private key has been displayed in the figure 2.7.

First the random generator is seeded. In order to generate a secure private key it is from great importance that the random generator is truly random and there should be enough entropy to create a 256 bit random number in order to generate a secure private key. After the random number has been generated it will be hashed through a hashing algorithm [3, 7].

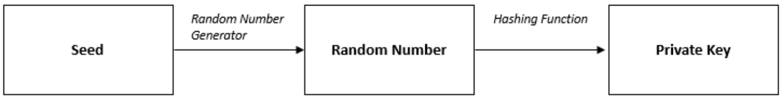


Figure 2.7: Overview of generation private key

2.4.4 Public Key

The public key is generated from the private key. The public key is constructed out of the private key via elliptic curve multiplication. In general all Blockchain based applications use a predefined set of parameters to define their elliptic curve. These parameters define a specific point on the elliptic curve, which is often referred to as the generator point [3, 7].

The generator point is used in order to calculate the public key. The public key is obtained by applying the elliptic scalar multiplication with the generator point and the private key. In equation 2.1 the computation of the public key is shown. Where P_k denotes the public key, P_{rk} denotes the private key and G denotes the generator point.

$$P_k = P_{rk} \circ G \tag{2.1}$$

The demonstration of the following example shows the ease of the forward calculation of the public key and the hardness of the inverse problem. Suppose the value of the private key amounts 129 than the public key can be computed within 7 steps by applying a combination of point doubling and point adding operations. The public key can be computed in 7 steps.

By applying 7 consecutive point doubling operations $G \circ G = 2G, 2G \circ 2G = 4G, 4G \circ 4G = 8G, 8G \circ 8G = 16G, 16G \circ 16G = 32G, 32G \circ 32G = 64G, 64G \circ 64G = 128G$ and one point addition $128G + G = 129G$ the public key can be computed in 8 steps. Where as computing the private key would cost at least 129 steps. Especially when larger numbers are used for the private key the problem of calculating the inverse becomes extraordinary difficult [16].

2.5 Transactions

In general the transaction protocol is of major importance for the Blockchain based applications. It relies on cryptographic securitization which enables the possibility for peers participating in the Blockchain network to establish transactions without the need of trusting each other [3].

The transaction protocol ensures correct generation of new transactions and the ability to verify these transactions by other peers within the network. The enforced cryptographic securitization method is applied by constructing digital signatures for the transaction [7, 9].

In general a transaction could be considered as a piece of data which has been provided with a digital signature. Whether this data resembles a monetary transaction between two peers within the network in the case of Bitcoin or a request to perform computations on the Ethereum platform it relies on the same principle.

2.5.1 Digital signature generation and verification

A transaction takes places between two addresses, the address of the payee and the payer. A transaction is a piece of data which typically consist out of information about the version of the software used of the Blockchain based application, a time stamp of the transaction, data which refer to the assets which are linked to the address of the payer and data which states the desired amount transferred and the address of the payee [3, 7, 9].

The payer who creates the transaction provides a digital signature with the transaction. This digital signature is created with the private key of the payer and a designated message with the data containing information about the specific transaction. The digital signature could be considered as a seal of the transaction which ensures authenticity and integrity of the transaction [7, 9].

The digital signature provides authenticity to the transaction since it has been generated from the private key of the payer. Which ensures the true identity of the payer since only the payer has access to his private key.

Integrity is enforced by the digital signature since it offers resistance to tampering with the designated message containing the transaction data [9]. If one would maliciously tamper with the data from the specific transaction the signature will become invalid.

If the signature is generated correctly, a peer could share the signature with other peers without revealing any details about the private key that has been used for generating the signature.

This feature of the cryptographic securitization method behind the digital signature imposes an important property of Blockchain based applications since there is no need for peers to trust each other and to communicate with each other over secured channels. Opposed to credit card information for example where it is crucial to have secured communication.

In order to understand the properties of the digital signature it is important how the signature is created. In the figure 2.8 the process is shown how the signature is created.

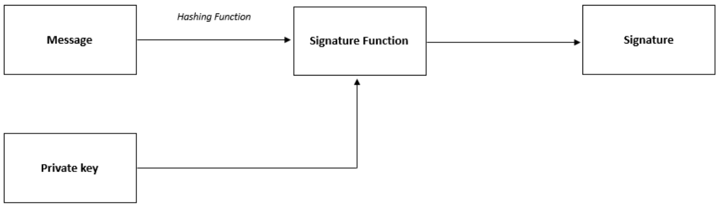


Figure 2.8: Overview signature creation

One could see from figure 2.8 that the digital signature is created from the message containing data of the specific transaction and the private key of the payer.

Before the message is inserted in the signature function a hashing function is applied on the message. By applying a hashing function integrity is ensured. If one would alter the message containing the transaction data only a single bit the outcome e.g. signature would be completely different due to the properties of the cryptography hash function [3, 9, 13]. As a result the signature would not be valid anymore.

In order to verify the digital signature of the payer. The payer sends his created signature and his public key across the Blockchain network. Other peers within the network have the ability to check the created signature with the public key of the payer. This procedure can be executed without revealing any details of the private key of the payer [8, 14].

2.6 Consensus and Mining

The Blockchain consists of a collective of technologies. One of these technologies is a mechanism which establishes consensus among the nodes participating within the network. The mechanism provokes consensus among all those different nodes about the current status of the ledger and the inclusion of new transactions within the ledger [1, 3, 7].

In the majority of Blockchain based applications the mechanism consists out of four processes: Firstly, independent verification of new transactions by nodes participating within the network. Secondly, mining nodes aggregate newly created transactions into blocks by executing the mining protocol. Thirdly, independent verification of the newly created blocks by the the nodes participating within the network. Fourthly, recording validated blocks onto the ledger by reaching consensus on the current state [1, 3, 7, 9].

2.6.1 Independent transaction verification

If a node creates a new transaction it will broadcast the newly created transaction to its connected peers within the network. Once the other nodes receive the transaction they will verify whether the transaction complies with a specific set of rules. In the majority of Blockchain based applications these rules consist of a set of pre-eminent rules and a set of application specific rules. One could think of pre-eminent rules such as whether the transaction has a valid signature, if the assets included within the transaction truly belong to the creator of the transaction. The set of application specific rules can entail rules such as whether the data structure of the transaction is in the correct format, the transaction syntax is correctly applied or if transaction fee's for processing of the transaction are included [1,3,7].

If a node verifies the transaction according to the consensus rules and the transaction complies with the rules it will send the transaction to other connected nodes otherwise the transaction will be disregarded [3,7].

2.6.2 Mining

After a set of transactions have been approved by the verification process the mining process will commence. The mining is the process of the consensus mechanism which provides two important properties for Blockchain based applications. The mining process provides a resistance against fraudulent alterations of the ledger. And it provides an economic incentive for nodes, which participate in the mining process, to solely include valid transactions into blocks [1,3,7,17].

The majority of Blockchain based applications are based on a mining protocol known as proof of work protocol. The proof of work protocol is an algorithm which consist out of a mathematical puzzle where a solution to the problem can only be found by guessing a solution by trial and error. Mining nodes compete with each other in order to find the solution of the proof of work algorithm. Through execution of the mining protocol new blocks are created and the mining nodes are economically rewarded for providing their computational power when the protocol has been executed successfully [1,7].

In order to gain a full understanding of the mining protocol in general it is important to understand how blocks are structured. A block is a collection of recent transactions which haven't been recorded in previous blocks yet. Blocks are created by successful execution of the mining protocol. In the majority of Blockchain based applications a block consists out of two parts the header and the body [3,7].

In figure 2.9 an schematic representation is shown of the creation of a block. A set of verified transactions are compiled into a block by execution of the mining protocol. As shown in the overview a the Block consists out of a header and data which contain information about the transactions included. In general the header is the most important part of the block for a typical Blockchain based application [3,7,10].

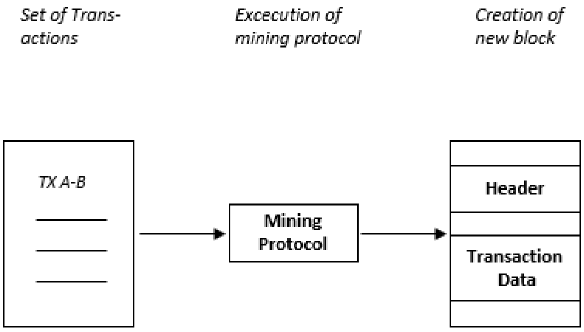


Figure 2.9: Simplistic overview of creation block

The most common mining protocol for Blockchain based applications, known as proof of work, is based on cryptographic hashing functions. The hashing function is a function which converts data into a fixed size regardless of the length of the input. The input of data and the result of the hashing function are referred to as the message and the hash respectively. In the ideal case hashing functions, which are used for cryptographic purposes, have the following properties [3, 7, 13]:

It should be computationally infeasible to calculate the message from any given hash nor should it be possible to deduce patterns in order to predict the message for any hash. Another important feature of the hashing function is that a small change in the message would result in a complete different hash. The hashing function should be deterministic meaning that hashing a particular message would always yield the same hash neither should it be possible calculate the same hash from two different messages [13, 18].

The proof of work algorithm consists out of applying a hash function repeatedly on the header of the block. The mining node selects a set of approved transactions and will start constructing the header. In general the header for a typical Blockchain based application stores data such as a reference to hash of the previous block, nonce, merkle root, target, time stamp of block creation and information, used version of software [7, 10, 13]. An overview of a typical header is shown in figure 2.10.

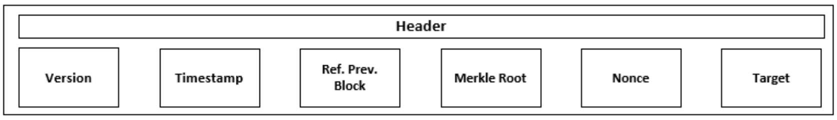


Figure 2.10: Simplistic overview of header

At the start of the proof of work protocol the mining node will construct the header. The header can be divided into a static part and a dynamic part during the mining process. The nonce is considered to be dynamic while all other elements are static. The nonce is an integer which will be adjusted during the mining process until a solution is found for the proof of work algorithm. The merkle root is a compressed string of all transaction data included [3, 7, 10].

A link is established with the previous block by including the hash of the header of the previous block. The target denotes a measure for the current difficulty. General information such as time of creation and specific software type used is also included in elements of the header [3, 7, 10].

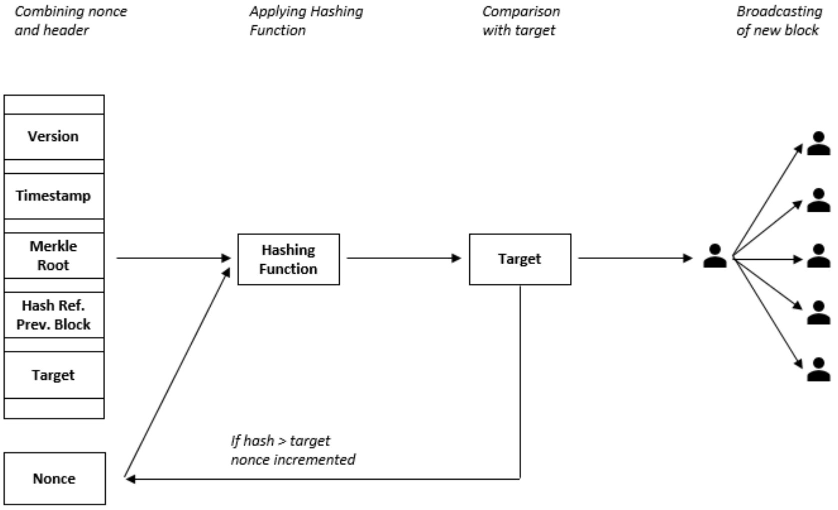


Figure 2.11: Overview proof of work algorithm

In figure 2.11 an overview is shown of the proof of work algorithm. Once the mining node has constructed the static part of the header it will be combined with the nonce. After applying the hashing function the outcome will be compared with the target. The goal of the proof of work algorithm is to find a lower numerical value of the hash than the target [10].

After comparison of the numerical value of the hash and the target there are two possible outcomes. The mining node could either find a nonce which provides a solution to the proof of work algorithm. Then the mining node has created a valid block and will broadcast it to the other nodes within the network. Or the numerical value of the hash exceeds the target and the nonce will be incremented. In general the mining process for Blockchain based applications is computationally exhaustive and takes a lot of attempts in order to find a solution [3, 7, 10].

The numerical value of the target determines the difficulty of creating new blocks. In general Blockchain based applications make use of target adjustments in order to maintain the mean time of creating a block constant. Increasing or decreasing of the difficulty is done in order to ensure stability due to variations in total computational power of all mining nodes.

The described properties of a cryptographic hashing function such as that a change of a single bit of the message leads to a complete different hash and that it is not possible to deduce patterns in order to predict the hash from a given message are exploited in the proof of work algorithm. Completely different hashes are produced by incrementing the nonce only a single bit until it provides a solution for the proof of work algorithm. Because it not possible to predict hash values for a given message nor calculate a message for a given hash value the only manner to find a solution for the proof of work algorithm is by trial and error [9, 13].

The manner how blocks are constructed and the properties of the cryptographic hash function in combination with the proof of work algorithm provides resistivitiy against fraudulent alterations of the ledger. Links are established between blocks by including the hash of header of the previous block into the header of subsequent block. By incorporating these hashes of previous headers the database structure of the ledger takes the shape of a chain of blocks [10], this is shown in figure 2.12.

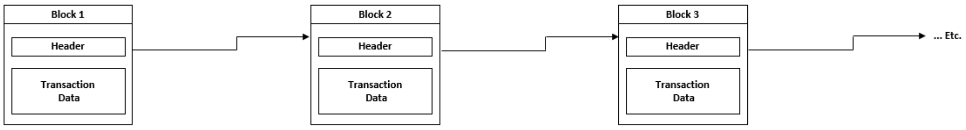


Figure 2.12: Display chain of blocks

The hash of the header contains specific information about transactions which is stored in a compressed form known as the merkle root. Suppose an adversary would want to include a malicious transaction for personal gains in block 1 of figure 2.11. It would result in a change of the merkle root hence a alteration has been made to the transaction data. Subsequently this would change the hash of block 1 due to properties of cryptographic hashing function and therefore the nonce of block 1, which proved to be a solution for the proof of work algorithm, turns out to be invalid [3, 7, 10].

The inclusion of the hash of the header of the previous block would lead to a changes in the headers of subsequent blocks resulting in invalid nonces of these consecutive blocks. This mechanism raises resistance to fraudulent alterations once data is included on the ledger. The nonce can be defined as a seal which breaks if one would tamper with the data and the structure of the blocks ensures breaking of all the nonces of subsequent blocks.

By engaging in the mining process mining nodes are economically rewarded for dedicating their computational power. In the majority of Blockchain based applications there are two types rewards. A reward is received when the mining node creates a new block hence finding a solution to the proof of work algorithm. In general this reward introduces the creation of new coins linked to the specific Blockchain based application. This reward is often referred to as the coinbase reward.

The other reward is received as transaction fees of the processed transactions. Transaction fees are determined by the issuer of the specific transaction, however in general these fees are standardized by the used software of the wallet. Mining nodes can decide whether to execute transactions for a given fee [3, 7].

Mining nodes are economically incetivized to solely include valid transactions. For the majority of Blockchain based applications the coinbase reward is paid out with a delay. After creation of the block the mining node will broadcast the block. The other nodes within the network will verify whether the transcations included in the block are valid. The coinbase reward is only paid out upon creation of valid blocks if the block turns out to be invalid the block will be rejected and the mining node has wasted it's spent energy on engagement in the mining process.

2.6.3 Independent block verification

After creation of a new block the mining node will broadcast the block to it's connected nodes within the network. Upon receipt of the new block the nodes will independently verify the block if it complies with the consensus rules. In the majority of Blockchain based applications the consensus rules consists out of rules such as whether syntax of the block is valid, the solution to the mining process is verified, the data structure of the block is correct, if the size of the block does not exceed the limitations and if all transactions within the block are considered to be valid [9].

Only when the block is considered to be valid the peers will send it to other peers within the network for verification. Therefore only valid blocks propagate through the network. The rationale behind the independent verification of the blocks ensures that mining nodes can't act in a fraudulent manner.

2.6.4 Consensus about the current state of the ledger

The last step of the consensus mechanism consists out of reaching consensus about the current state of the ledger. While mining nodes compete with each other in finding a solution to the proof of work algorithm it often occurs that two nodes find a solution to the algorithm at the same time. Both mining nodes will broadcast the newly created block to it's connected nodes. After the node has received the new block it will verifies the block and assembles it onto the existing chain of blocks [3, 7, 9].

Because Blockchain based applications are communicating over a peer to peer network which is decentralized by nature it takes time for the blocks through propagate through the network. As a result, some nodes might have different versions of the chain of blocks. Consensus has to emerge among the nodes within the network about the valid chain of blocks.

Suppose that two mining nodes discover a solution to the proof of work algorithm within a short time. Both mining nodes will broadcast their valid blocks through the network. After receiving the block each node will assemble the block onto the existing chain of block. As time passes nodes start receiving both blocks and will create a branch onto the existing chain of blocks. This is shown in figure 2.13.

As a result, there are temporarily two versions of the ledger. Mining nodes which received block *4a* first will start the mining protocol in order to find a solution for the proof of work algorithm hence building on top of branch *4a* and mining nodes which received block *4b* will try to build on branch *4b*.

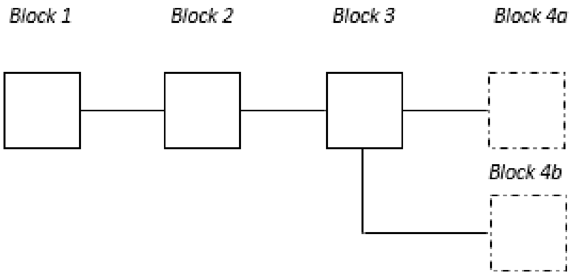


Figure 2.13: Display of a side branch

Suppose that one of the mining nodes which worked on extending branch *4b* finds a solution to the proof of work algorithm and broadcasts his newly created block. Nodes which received block *4a* first will try to assemble block *5* onto block *4a* and will notice it corresponds to block *4b*. This is shown in figure 2.14.

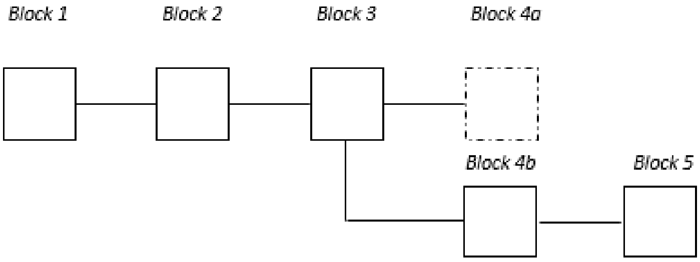


Figure 2.14: Display of a side branch

Consensus is achieved by the nodes within the network by adopting the chain with the most solutions of the proof of work algorithm as the main chain of blocks. The chain with the most solutions of the proof of work algorithm is considered to be legitimate because it possesses the most spent computational power [3, 7, 9]. As a result of the fact that the majority of mining nodes have spend their computational power working on this chain. In the example this would be inclusion of block *4b*.

Chapter 3

Current and Future grids

This chapter will identify the potential area's within the smart grid where the Blockchain can be applied. Section 3.1 given an overview how the electrical power system is structured in the Netherlands and will explain the various roles of different parties involved within Dutch power system. Section 3.2 will introduce several case studies which will be used throughout the Thesis.

3.1 Overview electrical grid Netherlands

The first Dutch power plant which produced electrical energy was build in 1886 in Rotterdam. In 1886 the first electrical power plant possessed an installed capacity of 59 KW and the main purpose of the power plant was to provide electrical energy for 350 lamps [19]. In order to transport the produced electrical energy to the load a transmission grid was built. In comparison to 1886 our current electrical power system has evolved quite a bit. Our current grid of our electrical power system has a total length over 300.000 km and facilitates the transport of 120 billion kwh [19, 20].

In essence the electrical power system is designed to transport electrical energy in a reliable and economical fashion. Since the beginning of the development of electrical power systems in the nineteenth century the performance has increased significantly through the improvement of technology resulting in increased safety, lower failure frequencies, increased reliability etc.

However, the basic physical principle that underpins how the electrical grid works has not changed. The electrical grid has hardly any capability to store energy e.g. electricity. This introduces the necessity for the electrical power system to be continuously in balance hence the generated electrical energy needs to be consumed by the loads. Therefore a balance should be remained at every instant within the electrical power system between generated energy and consumed energy [21]. One could imagine it as a scale as shown in figure 3.1.

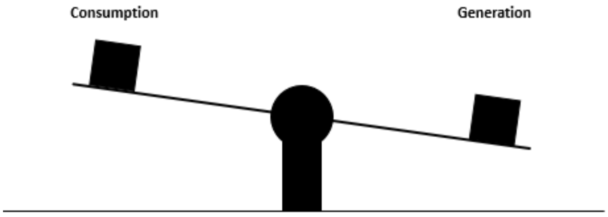


Figure 3.1: Balance between consumption and generation

Small disturbances may cause to small variations in the load-generation balance which resulting in varying voltage level and frequency of the electrical power system. These minor variations of the voltage and frequency level are allowed within restrictive limits. The majority of these minor disturbances can addressed through the capability of large generators to store a relatively small amount of energy by exploiting their inertia [21].

However, if larger disturbances occur corrective measures have to be applied. Otherwise these disturbances might cause large voltage and frequency fluctuations resulting in partial or even complete blackouts of the electrical power system e.g. leading to large economical damages for society [21].

The current electrical power systems such as the one present in the Netherlands is primarily designed to facilitate the transportation of produced electrical energy by large power plants to consumers. The majority of electrical energy produced is generated at these large power plants using fossil fuels as energy source such as coal, gas and oil [22].

In figure 3.2 a basic overview is shown of the current electrical power system present in the Netherlands . As one can see electrical energy produced by the power plants is transported via the electrical grid to the consumers.

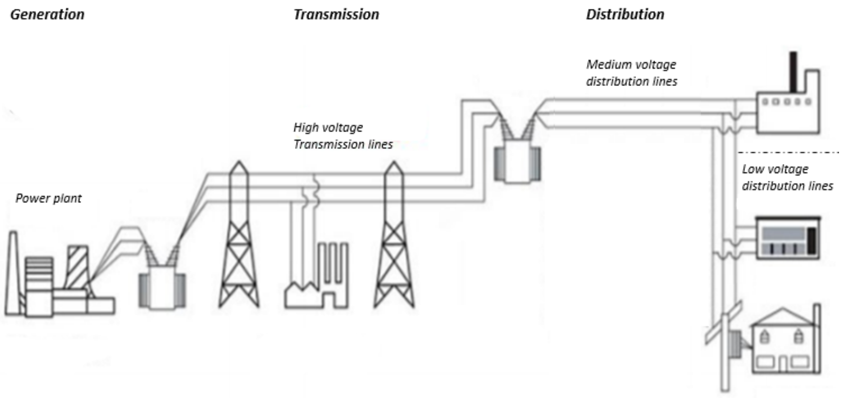


Figure 3.2: Overview structure grid

The electrical grid consists out the transmission grid and the distribution grid. The main purpose of the transmission grid is to transport electrical energy produced by these large power plants over long distances before distribution of the electrical energy to the consumer.

In order to minimize transmission losses the transmission grid is operated at very high to high voltages. The voltage levels which are commonly used in the Dutch transmission grid are 380 KV, 220 KV, 150 KV and 110 KV [22, 23]. In general the transmission grid which consists out of cables and overhead lines are owned and operated by the transmission system operator [22]. In the Netherlands the transmission system operator is TenneT.

When the electrical energy is transported on regional level via the transmission grid it will be delivered to the end consumer via the distribution grid. The primary purpose of the distribution grid is to transport the electrical energy to various end consumers.

The distribution grid is operated at medium voltage levels, commonly used voltage levels range from 50 KV to 10 KV [23]. Depending on the imposed load by the consumer the consumer is connected at a specific voltage level. Larger consumers might be connected to a voltage level ranging up to 15-25 KV whereas households are connected at a low voltage level of 400V.

In general there could be three grid structures distinguished which are used to connect loads with the distribution grid. These different grid structures consists out of a radial, looped and meshed grid structure.

In figure 3.3 an overview is shown of the different types of grid structures. Comparing the different grid structures with each other there is a trade of between economical cost of construction and reliability of the connection of the different grid structures. In a radial grid structure multiple loads are connected via a single branch. It offers the most economical solution concerning the cost of construction, however it is limited in terms of offered reliability of the connection. If a fault occurs at the beginning of the branch of the radial configuration multiple loads are cut off.

The looped grid structure offers a more reliable connection. If a fault occurs at the beginning of the loop only a few loads will not be supplied. The economical cost of construction is higher compared to radial grid structure but less than the meshed grid structure. The meshed grid structure is the most expensive grid structure however it offers the most reliable connection compared to the other grid structures.

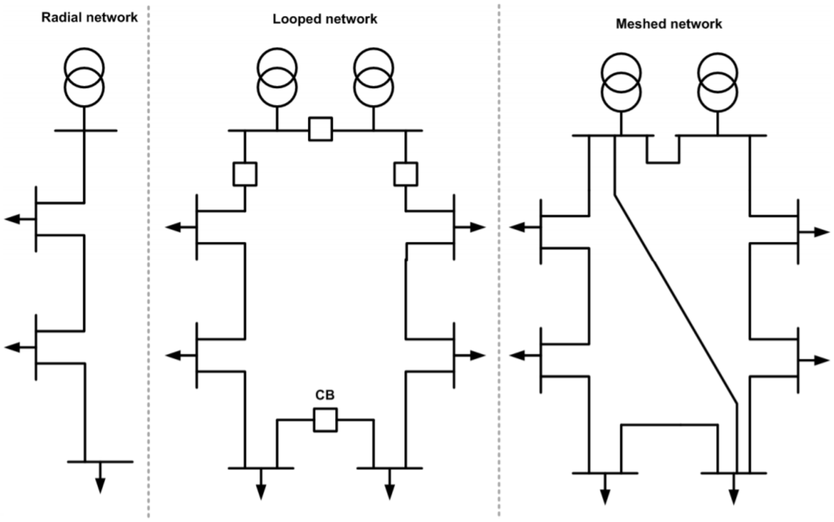


Figure 3.3: Overview types of grid structures

In the current Dutch electrical power system there are various actors who fulfill different roles within the electrical grid and cooperate together in order to provide electricity to different customers in a secure and reliable fashion. These different actors consist out of electricity production companies, energy suppliers, transmission system operator, distribution system operators and customers.

The electricity production companies own and operate electricity production facilities in order to produce electricity and supply the loads connected to the power system. These electricity production companies interact with energy suppliers on the wholesale electricity market where trade is established by electricity production companies offering their produced electricity and the energy suppliers having the opportunity to buy electricity [22].

The energy suppliers deliver energy to the end consumers. These energy suppliers buy the energy at the wholesale market and deliver it through the transmission and distribution network to their end consumers. However, it is also possible for energy supply companies to produce electricity by themselves as well examples in the Dutch electrical power system are companies such as Nuon, Essent [22, 24]. The key role of energy suppliers is to estimate and predict the requirement of electricity of their end consumers because they are responsible for the imbalances caused by their end consumers within the electrical grid [24].

In figure 3.4 a schematic overview of the dutch electrical energy markets is shown. The entire Dutch electrical energy market consists out of three markets: the forward and future market, the day a head market and the intra day market [22].

Figure 3.4: Overview of Dutch electrical energy market

At the future market long term bilateral contracts are traded which induces the obligation to either produce a given amount of electricity at a certain point in the future or buy a certain amount of electricity in the future. Usually these long term contracts are traded one to a few years before the actual delivery of the electricity. These traded contracts are legally binding therefore both parties have to fulfill the contract meaning that electricity production companies have to deliver the defined amount of electricity and energy suppliers have to pay the defined amount of money [22].

At the day ahead market energy suppliers and electricity production companies can buy and sell electricity 24-36 hours in advance for actual delivery. Electricity production companies and energy suppliers revise their forecast of demand and generation and have to opportunity to adjust their balances by buying or selling electricity at the day ahead market [22].

At the intra day market electricity is traded up to short till ultra short before actual delivery. Electricity can be traded until gate closure which occurs 5 minutes for actual delivery. After gate closure the transmission system operator accesses whether the electrical power system is in balance [22].

In figure 3.5 an overview is shown of the interaction between the different actors within the Dutch electrical power system. As can be seen in step 1 and step 2 in the figure electricity production companies, energy suppliers and very large customers interact with each other at the wholesale electricity market.

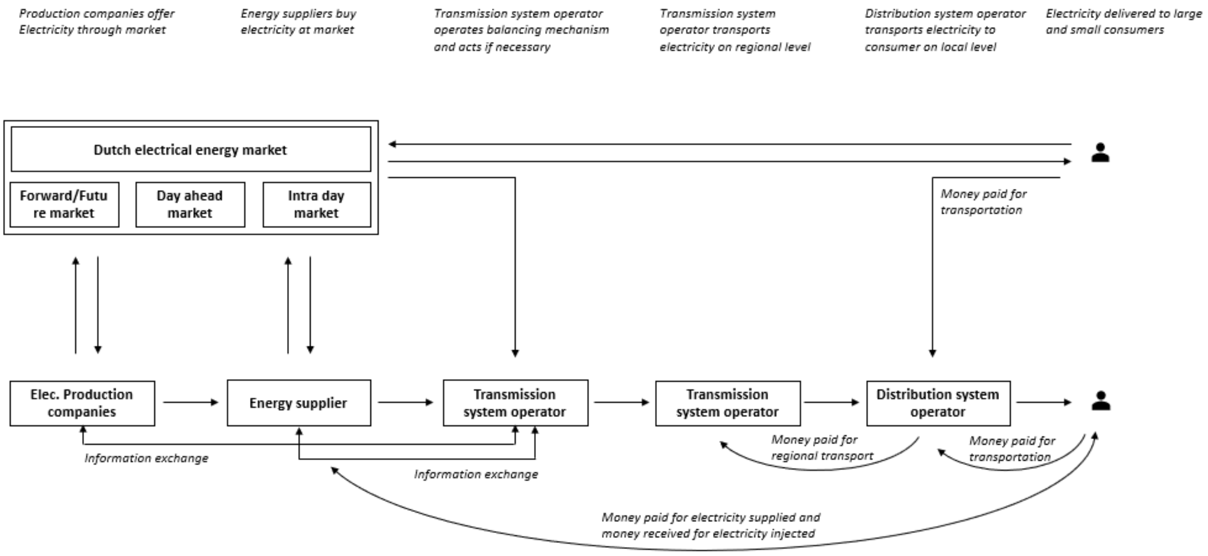


Figure 3.5: Overview of Dutch electrical power system

In step three of the figure one of the core responsibilities of the transmission system operator have been depicted which encompasses the responsibility of maintaining a balance between load and generation at during every instant in the electrical power system. While energy suppliers, electricity production companies and large customers establish electricity transactions with each other the transmission system operator, which is Tennet in the Netherlands, operate a balancing mechanism in order to maintain a balance of load and generation with the electrical power system [22, 24].

The day before the actual delivery of electrical energy the energy suppliers, electricity production companies and the large customers have to fill in a specific form called the E-program. These parties state via this E-program how much electricity they are going to produce or consume from the electrical power system during specified intervals throughout the day [22, 24].

When parties deviate from their stated E-program either electrical energy has to be used to compensate for the difference if their is a shortage or production has to be withheld if their is a overbalance. Parties who deviate will be economically penalized by the transmission system operator [24].

Therefore, they have an incentive to stick to their stated program. Because energy suppliers are responsible for the imbalances caused by small customers it is crucial for them to estimate and forecast the required demand of these small customers accurately. In general energy suppliers buy the bare electricity usage at the forward market from the electricity production companies and revise their position a day ahead to make more accurate predictions and to prevent penalties due to imbalances.

However, imbalances do occur either due to unforeseen circumstances such as weather fluctuations or due to outages of electricity production facilities etc. Therefore, the transmission system operator possesses several reserve capacities to reestablish balance within the electrical power system. There are three reserves of electrical energy withheld by the transmission system operator which could be distinguished: the primary reserve, the secondary reserve and the tertiary reserve [22].

The primary reserve is used via automatic control loops in order to restore frequency deviations due to imbalance within thirty seconds when a disturbance has occurred. Primary reserve capacity is bought by the transmission system operator in weekly auctions from electrical energy production companies [24].

If the unbalance remains and shifts towards either a shortage or abundance of electrical energy within the power system the secondary reserve will be initiated. The secondary reserve is established by the transmission system through annually contracting large consumers and electricity production companies which are able to increase production or dispatch a certain amount of their load. These companies have to keep a certain reserve and receive an economical compensation in return [22].

If their is a shortage of electrical energy within the power system electrical production companies are asked to offer capacity and if their is an abundance large consumers will be asked to dispatch their load partially by the transmission system operator. Non contracted parties are also able to bid in on a dispatch or to offer extra capacity however they do not receive a fixed compensation and they do not have to reserve any capacity [22].

In case of emergency if the unbalance remains present for a period longer than 15 minutes tertiary reserves are initiated. Tertiary reserve is procured in a similar fashion as secondary reserve capacity [22].

In step four the other responsibility is depicted of the transmission system operator which is to facilitate the transmission of electrical energy within the grid on regional and cross border level. In the Netherlands the transmission system operates and maintains high voltage level connections of 110 KV and above. Some well known examples of international connections are Norned and Britned which are the connections with Norway and Britain but the Netherlands is of course also connected with neighboring such as Belgium and Germany [22, 24].

After transmission of the electrical energy on regional level the distribution system operator distributes the electrical energy to the end consumer via the distribution grid. The distribution operator pays the transmission system operator for transportation of electrical energy on regional level as shown in figure 3.5.

In the Netherlands there are currently eight distribution system operators who all have the responsibility to operate, maintain and facilitate the distribution of electrical energy in a specified geographical region of the Netherlands [22]. For example Stedin is the distribution system operator of South Holland.

In the last step the interaction of the smaller / larger consumer is shown within the electrical power system. The smaller consumer pays an amount of money to the specific distribution system operator depending on the geographical location for distribution of the electrical energy and has a contract with the energy supplier with specified rates for consumed electricity via his connection.

Smaller end consumers who produce electrical energy can net their production of electrical energy with their energy consumption. Effectively energy suppliers have to buy their electrical energy for the same rates as they would deliver their own energy. This is obliged by law and it is called the salderingsregeling. However, if production of the end consumer exceeds their consumption energy suppliers are obliged to buy excess energy at a rate of their choosing. Often this happens at discounted rates.

The larger consumers buy their electricity directly from the wholesale market and pay the distribution system operator for transportation of the electrical energy.

3.2 Defining case studies

In order to study the potential area's of application of the Blockchain within the smart grid it is necessary to define a number of case studies. These same case studies are used at a later stage in order to identify the advantages and technical challenges of implementation.

The case studies differ in the level of adoption of the Blockchain and the the functionalities it can provide with respect to the current and future grid.

The level of adoption of the Blockchain can be classified in: a fundamental adoption of the Blockchain and an enhanced adoption of the Blockchain. The fundamental adoption of the Blockchain involves the implementation of a decentralized trading infrastructure via the Blockchain. Where as the enhanced level of adoption of the Blockchain involves the creation of a decentralized computing platform by addition of computational capacity via the Blockchain.

By creating a decentralized computing platform via the Blockchain additional functionality could be offered compared to solely establishing a peer to peer trading infrastructure. Functionalities such as dynamic load shedding, dynamic pricing and more accurate predictions of energy demand and generation could be offered. These additional functionalities could be of great value to the current and future grid.

In figure 3.6 an overview is presented of the combination of different levels of adoption of the Blockchain and potential functionality. As can be seen four different case studies can be distinguished: the market case study, the metering case study, the applied knowledge case study and the control case study. Depending on the level of adoption of the Blockchain a variety of functionalities can be offered ranging from a basic to an advanced level.

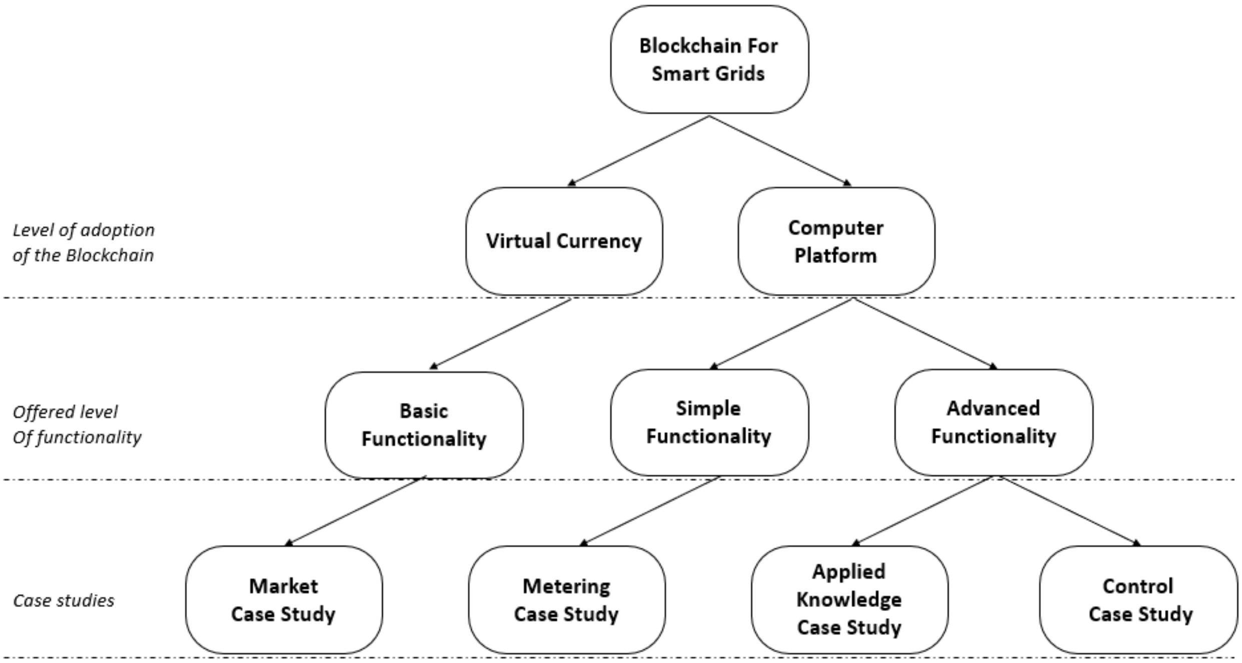


Figure 3.6: Overview level adoption of Blockchain and level of potential functionality

3.2.1 Market case study

The market case study is based on a fundamental level of adoption of the Blockchain. A basic functionality with respect to the current and future grid is offered by the establishment of a peer to peer trading infrastructure via the Blockchain. An overview of the established trading infrastructure is depicted in figure 3.7.

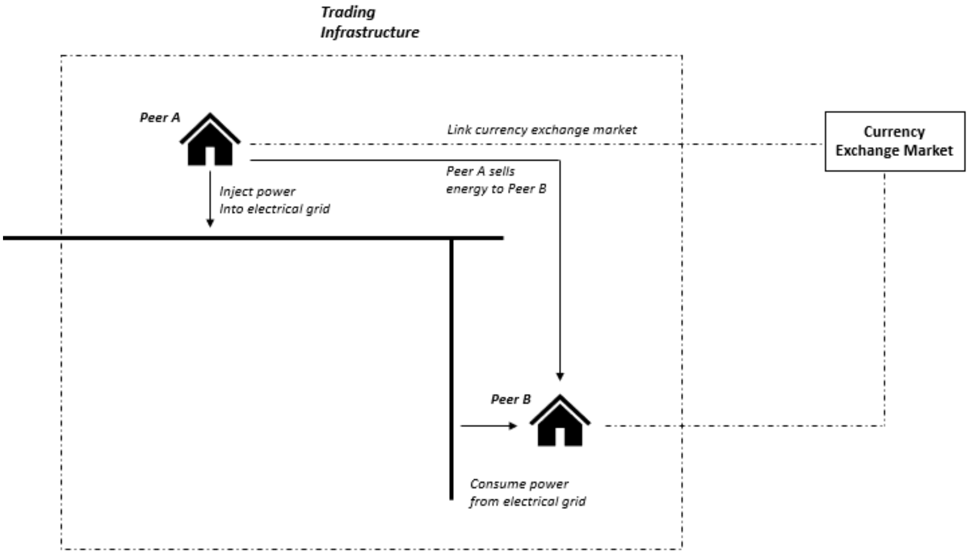


Figure 3.7: Schematic overview market case study

Through the application of the Blockchain a virtual currency is created which has a representation with a unit of electrical energy. Via the application of the Blockchain a peer to peer trading infrastructure is established where participants can make energy transactions with each other. This has been shown in figure 3.7 where peer A sells energy to peer B e.g. peer B buys energy from peer A.

Consumers and prosumers can engage in energy transactions with each other on small scale. If a consumer has a surplus of electrical energy available the consumer is able to sell this electrical energy by engaging into transaction with other peers within the Blockchain network and injecting this electrical energy into the grid. By selling this electrical energy at a specified price virtual currency can be earned by the prosumer.

Whereas consumers who have a deficit can buy electrical energy with virtual currency. This virtual currency can be bought or sold for Fiat currency at the currency exchange market as shown in figure 3.7.

This case study should be considered as the most primitive adoption of Blockchain within the electrical grid. Therefore this case study should be regarded as application of Blockchain as a pilot project. It is limited concerning the level of security it can provide to the participants.

3.2.2 Metering case study

The metering case study is relies on an enhanced level of adoption of the Blockchain. By addition of computational capacity to the Blockchain a decentralized computer platform is created in addition to the existing trading infrastructure. The metering case study involves using this computing capabilities in order to ensure a higher level of integrity and security for the participants involved within the peer to peer trading infrastructure.

In figure 3.8 a schematic overview is shown of the metering case study. Similar to the market case study a peer to peer trading infrastructure is established through application of the Blockchain and participants within this peer to peer trading infrastructure can establish energy transactions with each other.

Virtual currency can be earned by participants who sell electrical energy to other participants within the Blockchain network. This virtual currency is also linked to a currency exchange where participants can buy or sell this virtual currency for Fiat currencies.

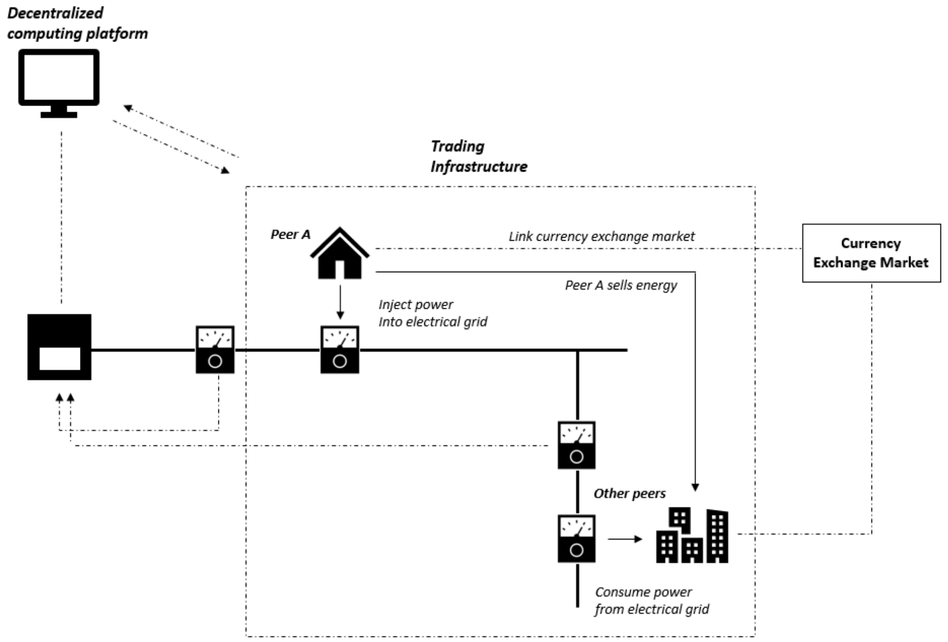


Figure 3.8: Schematic overview metering case study

Metering infrastructure is installed throughout the electrical grid in order to utilize the capabilities of decentralized computing platform. This metering infrastructure communicates with the decentralized computing platform as shown in figure 3.8. Through the installation of this metering infrastructure within the electrical grid and the utilization of the decentralized computing platform the ability is established for the participants within the Blockchain network to agree and reach consensus about the state of the system in a decentralized manner.

It has become possible for participants within the Blockchain network to check independently of each other whether a particular producer has truly injected electrical energy into the grid without selling it twice. This problem is classified as the double energy spending problem.

By developing such an infrastructure within the electrical grid security and integrity is ensured for the participants within the peer to peer market. Therefore this case study is suitable to be employed on larger scale. It should be considered as the first example of practical implementation of the Blockchain within the electrical grid.

3.2.3 Applied knowledge case study

The applied knowledge case study is based on an enhanced level of adoption of the Blockchain. Similar to the metering case study computational capacity is added to the Blockchain in order to create a decentralized computing platform in addition to the trading infrastructure. The applied knowledge case study involves utilization of the decentralized computer in combination with a smart metering infrastructure in order to gain knowledge about the electric grid and apply basic services for the electrical grid.

In figure 3.9 an overview is shown of the schematics of the applied knowledge case study. Similar to the metering case studies a peer to peer trading infrastructure is established through application of the Blockchain and participants are able to earn virtual currency by engaging in energy transactions with each other. This virtual currency is linked to an currency exchange were it can be bought and sold for Fiat currencies.

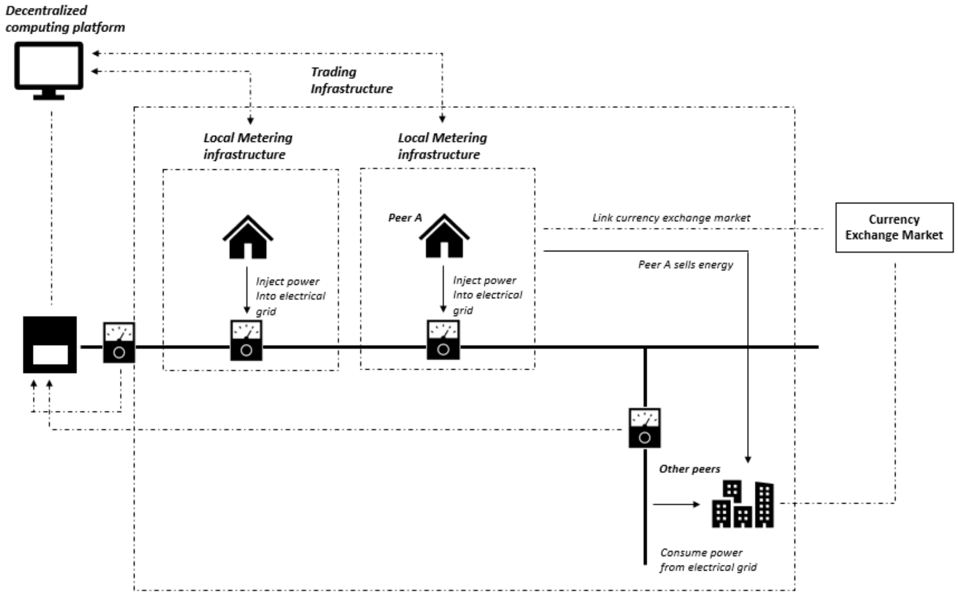


Figure 3.9: Schematic overview applied knowledge case study

Throughout the electrical grid a smart metering infrastructure is installed. However, in comparison to the metering case study the smart metering infrastructure is installed at local scale as shown in figure 3.9. This local smart infrastructure is installed at the connection of small loads within the electrical grid. For example, this local metering infrastructure is installed at the fuse board in houses or offices. All the smart meters within the peer to peer trading infrastructure communicate with the decentralized computing platform.

Through the installation of the localized smart metering infrastructure in combination with the decentralized computing platform more knowledge about various aspects of the electrical grid is gathered. The applied knowledge case study involves applicability of this knowledge in a limited range. The decentralized computing platform is able to process this information and provide services with respect to the electrical grid.

Transportation losses are calculated between peer to peer transactions in order to stimulate the consumption of locally produced electrical power, which would increase the efficiency of the existing infrastructure of the electrical grid. More accurate load forecasting can be applied in order to aid ancillary services. A basic initiation of demand side response pricing can be induced where the transmission system operator could offer a freely negotiated price in order to increase production electrical energy of prosumers.

The applied level case study should be considered as advanced scenario of the adoption of the Blockchain within the electrical grid. Whereas, the electrical grid it self has to change a significant amount as well in the form of the inclusion of a smart metering infrastructure on a local level. By implementing such an infrastructure within the electrical grid a more realistic peer to peer market will be created especially concerning the inclusion of transportation losses.

3.2.4 Control case study

The control case study relies on an enhanced level of adoption of the Blockchain. Similar to the applied knowledge case study and metering case study computational capacity is added to the Blockchain in order to create a decentralized computing platform in addition to the trading infrastructure. The control case study involves the utilization of the decentralized computational platform in combination with the localized smart metering infrastructure to integrate sophisticated features with respect to the electrical grid.

In figure 3.10 an schematic overview is shown of the control case study. The installed localized smart metering infrastructure will incorporate a more advanced level of sophistication compared to the applied knowledge case study. This localized smart metering infrastructure will be installed at the connection of small loads such as houses and offices. However, this localized metering infrastructure will also be incorporated at circuit level of this small loads.

The decentralized computing platform can enforce grid control through the localized metering environment. Grid users will specify cenrtain settings within their localized metering infrastructure which will determine the behavior of the applied grid control of the decentralized computing platform.

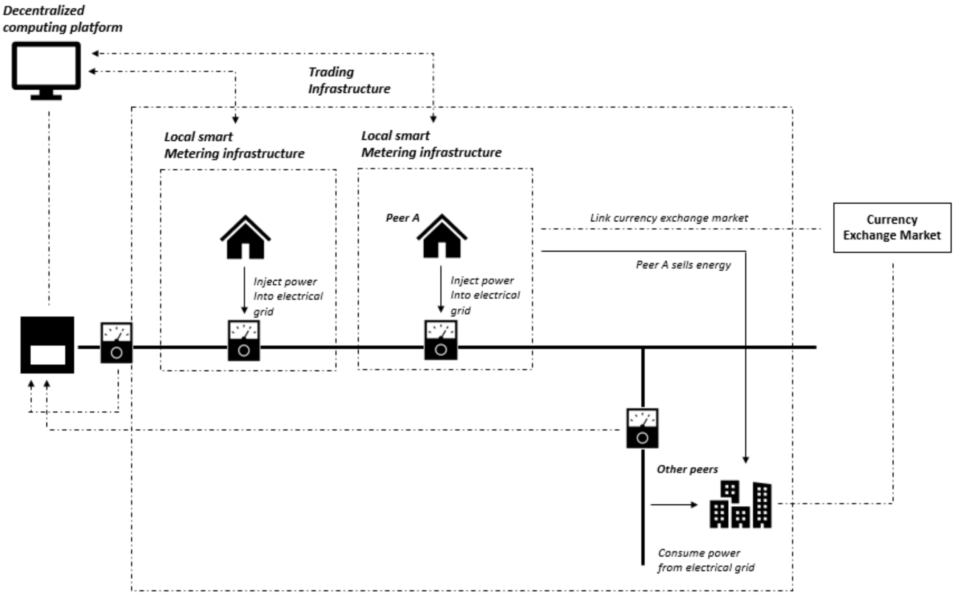


Figure 3.10: Schematic overview control case study

Through usage of the smart metering infrastructure and the computational platform more advanced services can be provided with respect to the electrical grid. One should consider functionalities such as enforcement of grid control through the smart metering devices of the load, real time prediction of energy demand and generation, dynamic load shedding where consumers specify via their smart metering devices the importance of specif loads and demand side pricing in order to manage a balance between demand and generation within the electrical grid.

One should consider the control case study as the most advanced implementation of the Blockchain within the electrical grid. Which would be able to support transmission system operators in their role.

Chapter 4

The advantages of the application of the Blockchain to smart grids

This chapter will discuss the advantages of application of the Blockchain to smart grids. Section 4.1 will discuss the advantages of application of the Blockchain for smart grids which are inherent to the characteristics of the Blockchain.

Section 4.2 discusses the advantages of applying the Blockchain based on the different case studies, which have been presented in chapter 3, such as the additional functionalities and their advantages for smart grids.

Section 4.3 will summarize the different advantages for the introduced case studies and provide an overview of the different advantages.

4.1 Advantages of characteristics of the Blockchain to smart grids

The application of the Blockchain to smart grids could offer various advantages to our current and future electrical power system. This section will discuss the advantages to smart grids which are specifically linked to the characteristics and the working principles of the Blockchain.

The case studies which have been introduced and explained in chapter 3 can be divided in two levels of adoption of the Blockchain: a fundamental level of adoption of the Blockchain and an enhanced level of the Blockchain. The fundamental level of adoption of the Blockchain involves the establishment of a decentralized trading infrastructure via the Blockchain. Where as the enhanced level of adoption of the Blockchain involves the creation of a decentralized computational platform in addition to the trading infrastructure.

The majority of the advantages to our electrical power system which are specifically linked to the characteristics and the working principles of the Blockchain arise from the established decentralized trading infrastructure.

The major advantages linked to characteristics and the working principles of the Blockchain with respect to the electrical power system are the decentralization of trust, increased security, increased resilience, increased transparency, increased scalability, less bureaucracy and increased computational capacity.

A large share of offered services in our current society base their added value upon acting as a trusted intermediary. These trusted intermediaries rely on centralized database structures in combination with the ability to alter these centralized database structures by acting as trusted intermediary. Whether this is the notary who alters land and housing titles in the central register after a sale or the retail division of the banking sector which is in essence a centralized database responsible for tracking the balances of their clients money and the specific bank will alter the balance after a money transfer.

The Blockchain provides the ability to participants within a decentralized network to establish transactions between themselves of particular assets without the requirement of trusting each other or even knowing each others identity.

For our current electrical power system the benefit of decentralizing trust is limited due to the fact that only a limited number of parties have access to establish electrical energy trades and the fact that these parties can all be trusted.

However, it would prove extremely valuable to our future electrical power system to manage small energy transactions if prosumers are allowed to offer their produced energy onto the markets. Without the requirement to build an expensive centralized architecture to manage these relatively small energy transactions.

The Blockchain offers increased security for the electrical power system. The applied cryptographic securitization combined with the consensus mechanism provides immutability of the data which has been incorporated in the Blockchain. Once an energy transaction has been included in the Blockchain it would be very hard to alter this transaction for illegitimate purposes or to delete the transaction resulting in a very secure and robust system.

The Blockchain also provides increased resiliency for the electrical power system. Due to the fact that every peer in the network contains a copy of the ledger their is an absence of a single point of failure compared to centralized data architectures which decreases the vulnerability for malicious attacks and therefore the electrical power system is more resilient.

For participants within the electrical power system either producer or consumers an trading infrastructure based on the Blockchain offers more privacy concerning valuable information such as their energy consumption behavior or other valuable details compared to centralized systems. Because there is no direct link between the identity within the Blockchain environment and the true identity of the specific consumer / producer.

The Blockchain increases scalability of the electrical power system, hence if an extra customer would be connected to the electrical grid there would be an negligible increase in complexity.

For both consumers and producers of electrical energy an trading infrastructure based on the Blockchain would offer increased transparency within the electrical power system about prices paid for consumed and produced electrical energy.

Through the adoption of an enhanced level of the Blockchain a decentralized computing platform is created in addition to the trading infrastructure. When all the peers who participate within the network devote a share of their computational capacity the total available computational capacity is increased within the electrical power system.

In addition it increases resilience of the electrical power system because the computational capacity is fragmented rather than concentrated in one large computer. Therefore, it will decrease the vulnerability against malicious attacks which increases resilience of the electrical power system.

4.2 Advantages of implementation of case studies

This section discusses the different advantages of the implementation of the case studies, which have been presented in chapter 3. The offered functionalities will be discussed after implementation of the four case studies i.e. the market case study, the metering case study, the applied knowledge case study and the control case study.

4.2.1 Market case study

The implementation of the market case study in the existing grid as shown in figure 3.4 leads to the creation of a small scale peer to peer trading market for end consumers. The new overview of the electrical grid is shown in figure 4.1.

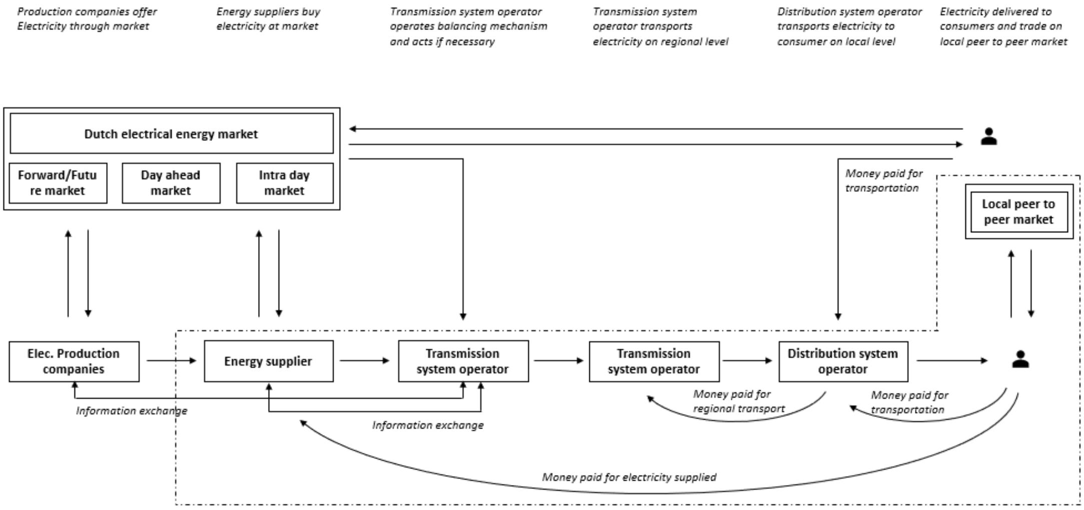


Figure 4.1: Overview of implementation market case study in Dutch electrical energy market

As shown in figure 4.1 a new peer to peer market has been created due to the implementation of the market case study. At this peer to peer market consumers and prosumers can establish energy transactions with each other.

In the current electrical power system in the Netherlands prosumers have the possibility to sell their excess of produced to their energy supplier at retail prices which is enabled by the salderings regeling. However, the salderings regeling which is enforced by the Dutch government will not offer a sustainable solution in order to handle and promote current and future generation of electrical energy of consumers.

Therefore, a local peer to peer trading infrastructure would offer the solution in order to manage the increasing amount of prosumers. As a promotion of the peer to peer market the government could decide not to tax energy bought by peers participating on this market. Therefore, it will be likely that prosumers will benefit due to the fact that they will be able to sell their excess of electrical energy at fair rate.

Consumers will benefit as well of the newly established trading infrastructure because they are able to buy electricity at discounted price compared to the retail electricity rates of the energy suppliers. This small scale peer to peer trading infrastructure allows consumers who are environmentally conscious to buy electrical energy of renewable sources such as electrical energy produced of the solar panels of their fellow neighbor.

Energy suppliers will benefit from the new implementations that they will not be obliged to buy back excess electrical energy of prosumers who generate more electricity than their energy consumption. However, sales of electrical energy to other consumers might decrease due to increased production of this group of prosumers.

4.2.2 Metering case study

An overview of the implementation of the metering case study into the existing Dutch electrical power system is shown in figure 4.2. The implementation, as depicted in the figure, results into a fully Blockchain operated electrical energy market where consumers, prosumers and electricity production companies can buy and sell electrical energy.

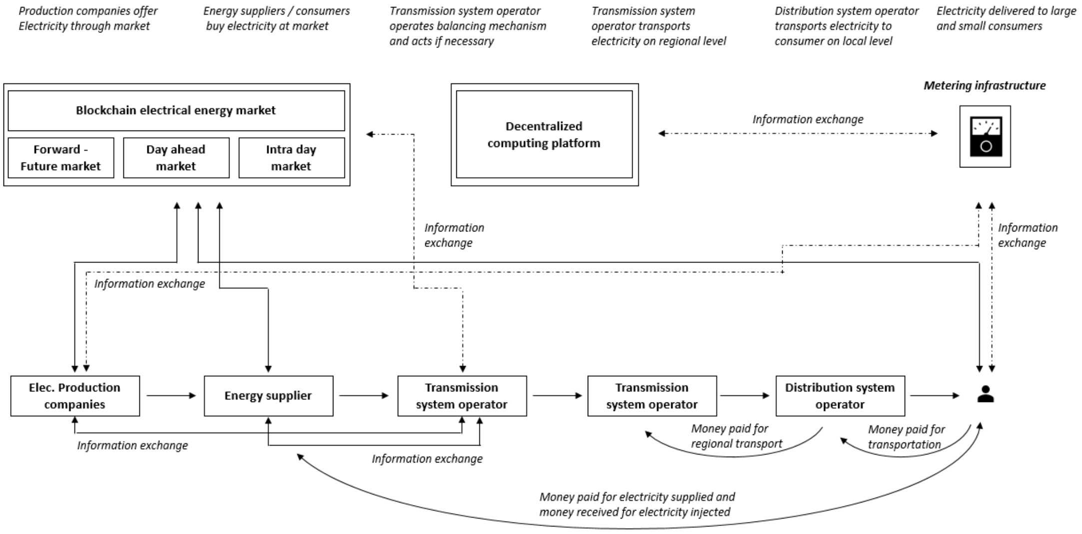


Figure 4.2: Overview of implementation metering case study in Dutch electrical energy market

Due to a fully Blockchain operated electrical energy market small consumers and prosumers are able to buy and sell electrical energy directly at the market place. In principle there would be no requirement for an energy supplier for consumers who directly participate on the electrical energy market. However, the energy supplier bears the responsibility of maintaining a balance between load and generation within the electrical power system.

It will be unlikely that small consumers are willing to accept the risk of facing high penalties of the transmission system operator because they have consumed more electrical energy than the amount they initially stated.

The major advantage of the implementation of the metering case study is the combination of the communication of the metering infrastructure installed throughout the electrical grid and the decentralized computing platform. Through this combination it has become possible for all participants within the Blockchain network to independently verify whether the sold electrical energy has truly been injected into the electrical power system.

Therefore, this feature enables to utilize the maximum potential of security offered of the Blockchain trading infrastructure which makes it employable on larger scale.

4.2.3 Applied knowledge case study

In figure 4.3 an overview is shown of the implementation of the applied knowledge case study into the existing Dutch electrical power system. Similar to the previous case study the implementation of the applied knowledge case study leads to a fully Blockchain operated trading infrastructure within the electrical power system. The implementation of the applied knowledge case study offers more advanced features with respect to our electrical power system such as more accurate demand forecasting, inclusion of transmission and distribution cost in electrical energy rates and a reduction of the role of the energy supplier.

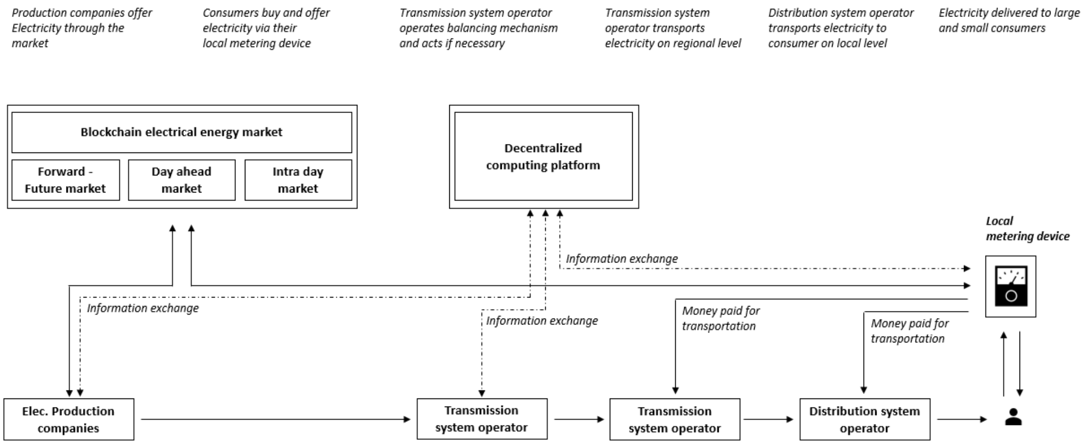


Figure 4.3: Overview of implementation applied knowledge case study in Dutch electrical energy market

As can be seen in the figure the role of the energy supplier is eliminated due to the implementation of a fully Blockchain integrated market combined with the decentralized computing platform. Consumers are aided by their metering device which communicates with the decentralized computing platform to buy and sell electrical energy. The metering device could act as automated agent to buy and sell electrical energy on their behalf.

Consumers will benefit from the new situation due to the implementation because consumers will participate directly onto the market without the interference of energy suppliers the electricity rates for consumers will be lower.

In comparison to the market and metering case study consumers are fully able to make the decision their self to buy electrical energy from energy producers. For example, specific consumers who solely want to buy electrical energy generated by renewable energy resources.

However, now that the energy supplier is eliminated in the electrical power system due to the implementation of the applied knowledge case study consumers and prosumers will face a form of responsibility in maintaining the balance of load and generation of the electrical power system.

The transmission system operator will operate grid control within the electrical power system. The transmission system operator will be assisted in order to do so by the computing platform. More accurate demand forecasting can be applied due to the increased amount of information gathered by the local metering infrastructure.

The local metering infrastructure is coupled to the decentralized computing platform in order to calculate the cost of transmission and distribution of the electrical energy. The cost of transportation of the electrical energy is determined by the losses occurred due to transportation and the usage of the transmission and distribution grid.

Consumers will pay transportation cost of electrical energy directly to the transmission system operator and distribution system operator. Based on the energy transactions of the specific consumers the computing platform can calculate the transportation cost of transmission on regional level and distribution of the electrical energy.

Therefore, consumers, prosumers and electrical energy production companies will have an economical incentive in order to buy and sell electrical energy on a local scale which will increase efficiency of the usage of the existing infrastructure of the electrical power system.

4.2.4 Control case study

An overview of the implementation of the control case study in the Dutch power system is shown in figure 4.4. As depicted in the figure this leads to certain thorough changes to our current electrical power system and the operation involved. Similar to the applied knowledge case study a fully operated Blockchain trading infrastructure is established due the implementation of the control case study. The implementation of the control case study provides more advanced and sophisticated functionalities with respect to our electrical power system such as demand side pricing, dynamic load shedding and controlling power flows.

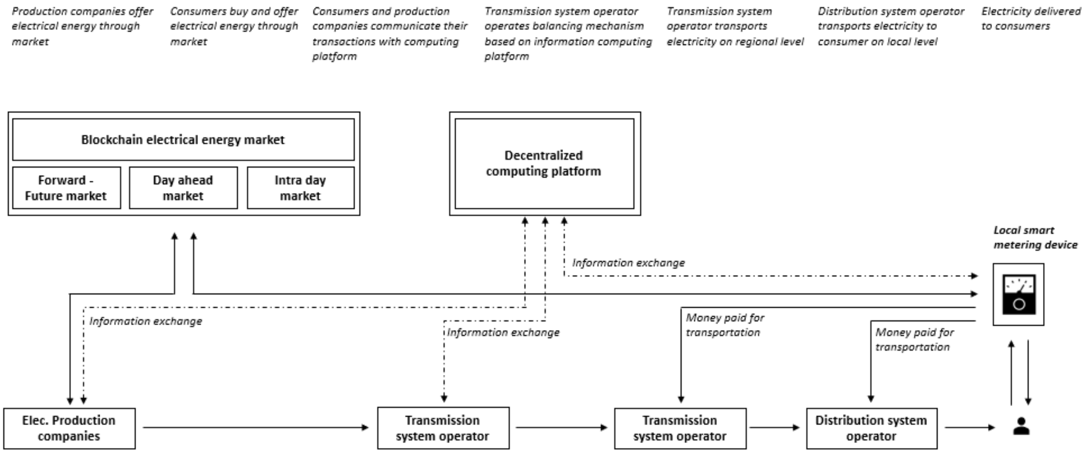


Figure 4.4: Overview of implementation control case study in Dutch electrical energy market

Consumers and prosumers offer and buy electrical energy via their local smart metering device. Similar to the applied knowledge case study this local smart metering device acts as an automated agent for the specific consumer or prosumer. However, in the control case study the automated agent can provide more functionalities.

The local smart metering device is installed at the connection of the specific load with the electrical grid and is interconnected to the sub circuits of the internal electrical system of the specific load.

This load could be an household, a large manufacturing facility or a shop. For example, the local smart metering device is installed at the fuse board of a household where it is connected to the internal sub circuits of the specific house for specific sub loads such as the washing machine etc.

Depending on type of consumer, the consumer can specify certain settings within the local smart metering device which will determine the behavior of prices paid for electricity, consumption window and enforced automated control.

The local smart metering device communicates the transactions with the decentralized computing platform. The consumer will face a form of responsibility in maintaining a balance between load and generation. However, the local smart metering device will automatically solve this problem for the consumer.

Similar to the applied knowledge case study consumers will pay the cost of transportation of electrical energy directly to the transmission system operator and distribution system. Hence the inclusion of transportation cost of electrical energy would lead to more efficient usage of the existing capacity of the electrical grid.

Consumers will pay transportation cost of electrical energy directly to the transmission system operator and distribution system operator. Based on the energy transactions of the specific consumers the computing platform can calculate the transportation cost of transmission on regional level and distribution of the electrical energy.

The transmission system operator will operate grid control and the grid protection within the electrical power system. In essence the role of transmission system operator could be eliminated by the decentralized computing platform. However, due to the importance of the activities and responsibility of the transmission system operator it would be more likely that the transmission system operator will be augmented by the decentralized computing platform.

Similar to the applied knowledge case study the transmission system operator will be assisted by the computing platform such as more accurate demand forecasting. But in addition more sophisticated functionalities can be provided with respect to grid control and protection of the electrical power system. It has become possible to enforce various control strategies such as inclusion of demand side pricing and dynamic load shedding rather than penalizing parties for differing in production and consumption. Which will be increasingly important due to the shift of conventional power plants to renewable energy resources intermittent characteristics.

Besides economical based control strategies the decentralized platform would be able to control the electrical energy power flows by the combining the decentralized computing platform with power electronics. Which would redefine our the manner how are current electrical grid is used. Which would enable the transmission system operator and distribution operator to actually deliver the bought electrical energy to the specific consumer.

It could also offer benefits for the transmission system operator with regards to operating protection scheme of the electrical power system. In the case of a congestion the electrical power flow could be rerouted or it could replace the requirement of protection equipment because the power flow could be adjusted in case of an overloaded line rather than using mechanical devices to insure overloading of lines within electrical grid and connected equipment.

The control of power flow could also be used in order to utilize transmission and distribution capacity within the power system more efficiently. By directing power flows through the transmission and distribution grid the capacity of the electrical grid can be used to it's full extend. The electrical energy could be rerouted along parts of the electrical grid which are not fully used based on their transmission / distribution capacity and heavy loaded lines can be spared by rerouting electrical energy

Another functionality which is enabled by the ability of directing power flows is to divide our existing electrical grid of the power system into AC micro grids. Rather than building micro grids based on hardware these micro grids could be constructed by directing the power flow which presumable would be cheaper to construct and it could be useful for is-landing and de-is-landing existing and new micro grids.

4.3 Summary

This section aims to provide an overview and context of the advantages of the different case studies. As explained in previous sections some advantages are specifically attributable to the Blockchain and its working principles and some advantages are derived from the provided functionalities. In figure 4.5 an overview has been presented of the advantages of applying the Blockchain per case study.

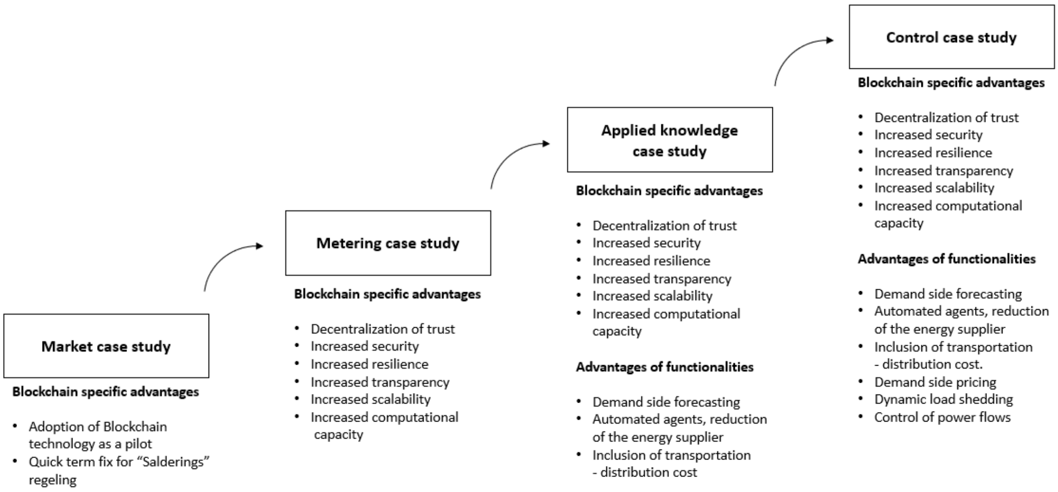


Figure 4.5: Overview advantages per case study

The market case study should be considered as a initial step in the adoption of the Blockchain within our electrical power system. The advantages which result from the implementation of the market case study are modest. The main advantage is the establishment of a small scale peer to peer trading infrastructure via the Blockchain where prosumers and consumers can trade electrical energy with each other.

The implementation of the metering case study is the first practical example of the adoption of the Blockchain within our electrical power system. A decentralized peer to peer trading infrastructure is established through application of the Blockchain in combination with a decentralized computing platform. By installing a metering infrastructure throughout the electrical grid of our power system security of the trading infrastructure is ensured. Due to the fact that security is fully ensured the implementation of the metering case study can be applied at large scale throughout the electrical power system.

All advantages which are specifically attributable to the trading infrastructure established by the Blockchain are applicable to this case study such as the decentralization of trust, increased security, increased resilience, increased transparency, increased scalability, less bureaucracy and increased computational capacity.

In provided functionality with respect to our electrical power system by exploiting the decentralized computing platform it is still limited.

The applied knowledge case study should be regarded as the first case study where the potential of the decentralized computing platform is explored with respect to our electrical power system. Similar to the metering case study the same Blockchain specific advantages apply. By using the computing platform various functionalities could be provided with respect to our electrical power system such as inclusion of transport / transmission losses within electricity rates, more detailed forecasting and an automated local agent which would buy electricity for consumers automatically leading to the elimination of the energy supplier.

The control case study should be considered as the most advanced adoption of the Blockchain. The full potential of the decentralized computing platform is exploited with regards to our electrical power system. Similar to the applied knowledge case study it enjoys at the advantages specically attributable to the Blockchain.

By using the full potential of the decentralized computing platform advanced functionalities can be provided with respect to our electrical power system such as control of power flows which would major impact on how the electrical power system would be controlled / protected in the future, control strategies like dynamic pricing and load shedding.

Chapter 5

The challenges of applying the Blockchain to smart grids

This chapter will discuss the various challenges of applying the Blockchain with respect to the Dutch electrical power system. Section 5.1 is intended to specify the challenges specifically linked to the Blockchain. Section 5.2 will discuss the technical challenges per case study to the electrical power system and the challenges specifically linked to each case study. Section 5.3 provides an overview of the various challenges per case study and potential solutions to the most eminent challenges will be discussed.

5.1 Challenges Blockchain

This section is intended to discuss the challenges specifically linked to the characteristics and working principles of the Blockchain. There are many potential advnatages to applying the Blockchain. However, since the Blockchain is a immature technology there are still various challenges to counter which are specifically linked to the characteristics and working principles of the Blockchain before it could be successfully implemented within the electrical power system.

The major challenges which have to be solved will be discussed in the following subsections of this section. The major challenges which have to be overcome could be classified in several themes such as issues regarding the consensus mechanism of the Blockchain, factors causing centralization within the Blockchain and issues regarding the peer to peer network of the Blockchain.

5.1.1 Issues regarding consensus mechanism of the Blockchain

There are several issues regarding the consensus mechanism of the Blockchain. One of the biggest challenges to overcome is the energy consumption of the mining protocol as part of the consensus mechanism of the Blockchain. The efficiency of the proof of work protocol i.e. is rather poor. The proof of work protocol is very effective in achieving consensus however it performs very poorly with respect to energy consumed per transaction.

The current annual energy consumption of the Bitcoin and Ethereum Blockchain is 52.5 Twh and 15 Twh respectively. The combined energy consumption of Ethereum and Bitcoin is already larger than the total annual energy consumption of a country such as Czech Republic. This shows how unsustainable the energy consumption is of these Blockchains which conflicts with the potential application of the Blockchain for the electrical power system to facilitate the integration of renewable energy sources for example.

In order to put the current energy consumption in perspective one could compare these Blockchains with a transaction service provider such as Visa which processes around 24 000 transactions per second and consumes 0.6 Twh on annual basis where Bitcoin processes around 3 transactions per second and consumes 52.5 Twh on annual basis. Effectively per transaction the Bitcoin Blockchain uses 700 000 times more energy per transaction making it very costly per transaction based on energy consumption alone. If capital cost are included of the mining equipment, which are specifically designed to execute the proof of work algorithm, the cost per transaction would be even higher.

Another challenge to overcome for the Blockchain attributable to the consensus mechanism is the limited benefits of increasing computational power with respect to security of the Blockchain. In essence it is correct that mining nodes provide security by devoting computational power to the Blockchain network. However, at some point if the available computational power in the network has reached a certain limit there is a decreasing border utility in adding more computational power. The additional computational capacity to the network just contributes into wasting energy since the performance of the Blockchain will not increase.

5.1.2 Factors causing centralization within the Blockchain

One of the key benefits of the Blockchain is the decentralization of trust within a peer to peer network. Due to the the Blockchain peers operating within this network have the ability to perform transactions without the intervention of third parties to secure trust. However, there are several factors which cause centralization within the Blockchain and could potentially devastate this key advantage of the Blockchain.

One of these factors causing centralization of the Blockchain is the clustering of devoted computational power through the deployment of mining pools. Mining nodes provide resilience against the so called 51 percent attack by devoting their computational power to secure the Blockchain. A 51 percent attack is considered if a party would control 51 percent of the computational capacity within the network and for this party it would be possible to rewrite the transaction history of the Blockchain.

However, in the case of the Bitcoin and Ethereum Blockchain the majority of independent mining nodes operate in mining pools where the mining nodes have clustered their computational power in order to maximize their economic returns. This offers the opportunity for mining pool operators to cluster their computational capacity of their mining pools and gain 51 percent of the computational power within the network of the Blockchain. Therefore, having the opportunity to perform a malicious attack. Besides that the clustering of computational power in mining pools leads to centralization of the Blockchain resulting in the fact that large mining companies and pools have control over the Blockchain.

On the other hand the clustering of computational capacity leads to possible stability issues of the security of the Blockchain. By clustering computational capacity it induces the risk of stability because large mining operators or mining pools are not able to stop their operations without the probability of one party processing more than 50 percent of the remaining computational capacity. This induces risk with regards to the stability of the security of the Blockchain.

The required space to store a full copy of the ledger of the Blockchain forms an another threat for the decentralization of trust of the Blockchain. For the most popular Blockchains such as Bitcoin and Ethereum the required storage for a full copy of the ledger amounts already over 100GB and 250GB. The initial release of Ethereum was only in 2015 and yet the required space already amounts 250GB. As time proceeds and more people start using the Blockchain the rate of growth of required storage space will only increase.

Running a full node is already impossible for mobile devices however it will become impossible for desktops and laptops as well because these devices in general only possess a hard drive with 500-1000 GB of storage space. Arguably the ledger could be stored on multiple data servers however than the peer to peer structure would be more or less converted into a traditional client server based structure and this would defeat one the core advantage of the Blockchain which is the decentralization of trust because these servers have to be trusted.

5.1.3 Scalability of the Blockchain

Another challenge which the Blockchain faces is issues regarding the scalability of the Blockchain. The main limitation regarding the scalability of the current design of the Blockchain is the limited transaction throughput.

In the current setup of a typical Blockchain it is not scalable. Because each node has to process the transactions the bandwidth of the total Blockchain peer to peer network is equal to the bandwidth of one node. The transaction throughput is limited to the bandwidth of the node with the least computational power available.

A choice is made in design of the Blockchain which compromises the scalability of the Blockchain, decentralization of the Blockchain and security. A choice is made in design of the Blockchain how much bandwidth is required to operate a node which leads to the consideration of a high or low transaction throughput resulting in a centralized / decentralized network since increasing the required bandwidth would exclude a certain number of nodes. In the majority of current designs of Blockchains there have been chosen to compromise scalability in favor of security and decentralization.

Besides that another issue regarding scalability of the Blockchain is that through the increasing number of nodes participating within the underlying peer to peer network the latency increases. The increasing latency within the peer to peer network reduces the available bandwith of the network resulting in a decreasing bandwith as the Blockchain grows through increasing participants of the Blockchain.

5.1.4 Governance of the Blockchain

For the current setups of the Blockchain challenges have to encountered regarding the governance of the Blockchain. In the ideal case each node who participate within the Blockchain votes in favor for the governance of the Blockchain by participating within the Blockchain resulting in the adoption of a decentralized governing model.

Major changes in the governance can be proposed by developers in the form of a hard fork of the Blockchain and the nodes can opt to either participate in the hard fork or opt to choose to participate within the existing Blockchain. However, the majority of participants within the Blockchain lacks the knowledge to make a clear judgment about the governance of the Blockchains resulting that the political power within the Blockchain belongs to developers and large mining companies who make decisions regarding the governance of the specific Blockchain. As a result the governance of current Blockchains such as Bitcoin or Ethereum does not differ that much of centralized governing models.

5.2 Challenges for the case studies

In chapter 4 the advantages of the implementation of the case studies have been explained with respect to our electrical power system. However, there are still numerous challenges which have to be countered before the proposed case studies could be successfully implemented in our electrical power system. This section is intended to discuss the various challenges per case study such as the technical challenges for the electrical power system regarding the implementation of the case studies and challenges specifically linked to the the implementation of the specific case study.

5.2.1 Market case study

Before the proposed market case study could be successfully implemented there are still several challenges to overcome. These challenges are mainly specifically related to the implementation of the market case study. Technical challenges with respect to the electrical power system are absent because the market case study is considered to be a pilot project and small in scale.

Challenges specifically linked to the implementation of the market case study

There are various challenges to counter which are specifically linked to the implementation of the market case study. These challenges mainly relate to the security of trading infrastructure, the stability of the Blockchain, the scale of the implementation of the market case study and the relationship between energy supplier and prosumer.

In general the market case study is intended as pilot project and as a first step in adopting the Blockchain as a technology within our electrical power system. Multiple small scale peer to peer trading infrastructures are established throughout the electrical power system by the Blockchain where peer can establish electrical energy transactions with each other.

A large challenge for the market case study is the presence of the double energy spending problem which compromises the security of the trading infrastructure. The double energy spending problem is classified as the problem that energy could be sold by a peer within the Blockchain network however it is not possible to verify whether this energy truly has been injected in the electrical power system. Therefore, would it be possible for malicious peers within the Blockchain network to sell electrical energy and consume the sold energy themselves. This compromises the security of the peer to peer trading infrastructures within the market case study however because of the local scale of the trading infrastructures malicious peers could be easily detected.

Another challenge which have to be countered is the billing of electrical energy by the energy suppliers in combination with the peer to peer traded electrical energy. The readings of the meters will not correspond to the delivered electrical energy by the energy supplier if the specific consumer has bought electrical energy on the peer to peer trading infrastructure. This could be solved by the fact that consumers / prosumers have to communicate the amounts of bought / sold electrical energy at peer to peer trading infrastructure with their energy supplier which could be settled with the billing of the energy supplier. However, energy suppliers could also play a role by developing these small scale Blockchain trading infrastructure where they could add value by providing the basic security against the double spending problem because they would have the overview and therefore could easily detect malicious peers.

A different challenge is formed due to the small scale of the peer to peer trading infrastructures. Because of the limited number of participants within such a peer to peer trading infrastructure the exchange rate of the virtual currency with fiat currency might fluctuate heavenly based on supply and demand. This could temporarily lead to overpricing and underpricing of electrical energy. Because it would be likely due to market forces that the virtual - fiat currency exchange rate would tend to move to the electrical energy rates offered by the energy suppliers.

Another challenges which have to be countered is that in the market case study energy suppliers are economically disadvantaged by prosumers who produce more electrical energy than they consume. In the current electrical power system prosumers who produce more electrical energy than they consume receive a discounted electrical energy rate however in the market case study the prosumer has the opportunity to either sell on the peer to peer trading infrastructure and to the energy supplier therefore maximize economical profit whereas the energy supplier is still responsible for the balance between load and generation of the specific consumer. Therefore it might occur that the energy supplier is penalized by the transmission system operator for re dispatch cost and the prosumer would maximize their economical returns by selling electrical energy at retail rates.

5.2.2 Metering case study

This section is intended to discuss several challenges regarding the implementation of the metering case study with respect to the electrical power system. The challenges can be categorized into two categories namely technical challenges with respect to the electrical power system and challenges specifically linked to the implementation of the metering case study.

Technical challenges metering case study

There are various technical challenges to overcome with respect to our electrical power system due to the implementation of the metering case study. The largest technical challenges arise from the physical connection between the electrical power system and the Blockchain such as securitization, information sharing, privacy.

The metering case study involves the installation of smart metering infrastructure throughout the entire electrical power system. The smart metering devices, which are installed at each connection of a load within the electrical power system, form the physical link between the electrical power system and the Blockchain. The installation of these smart metering devices does not form a challenge since these devices are already on the market and the Dutch government has made funds available for the replacement of analogue meters to smart metering devices.

The securitization of these smart metering devices forms a challenge to counter. These smart metering devices exchange information with the energy suppliers and the decentralized computing platform of the Blockchain. However, the vendors of these currently installed smart metering devices have not paid to much detail to securitization of their devices. The majority of these smart metering devices currently installed use dated communication protocols and lack proper encryption of their communication. Some manufacturers of the current smart metering devices have even used the same encryption key for the same series of meters which is a fundamental flaw in the securitization.

Therefore, the current smart metering devices are prone to attacks of hackers with potential disastrous consequences for consumers, energy suppliers and the electrical power system in general. Malicious attackers could fraud the smart metering devices causing energy suppliers to bill consumers for large amounts of electrical energy which they have not used. Theft of privacy related details concerning the consumption patterns of consumers could be misused for illegitimate purposes. Or even worse malicious attackers could attack multiple smart metering devices causing large outages which could harm the entire electrical power system on national level.

On the other hand malicious prosumers could hack their own meter to mimic that production e.g. delivering of electrical energy has taken place and sell this non produced electrical energy to other consumers within the electrical power system via the Blockchain which is classified as the energy double spending problem.

In general the smart metering devices form a critical link where the Blockchain trading infrastructure is connected with the electrical power system. In order to guarantee proper operation these devices should be adequately secured with respect to the information technology aspect and the hardware security in order to prevent malicious alterations to these devices.

Challenges specific to the implementation of the metering case study

For a successful implementation of the metering case study there are several challenges to overcome specifically linked to the implementation of the metering case study within the electrical power system. These challenges relate mainly to structural changes due to the implementation of the metering case study with respect to privacy infringement, responsibility of energy suppliers and the required processing power of the decentralized computing platform.

The metering case study involves the application of the Blockchain in order to establish a fully Blockchain operated electrical energy market combined with a decentralized computing platform. A large challenge to overcome is the required transaction capacity for a successful implementation of the metering case study. The required transaction capacity in the metering case study is mainly caused by the prosumers who in general establish small energy transactions. In the Netherlands there are around 400 thousand prosumers. In order to make a rough estimate it is assumed that electrical energy is traded in time intervals of 15 minutes. Under this assumption in worst case scenario the system needs to be able to handle circa 450 transactions per second.

Current Blockhains such as Ethereum and Bitcoin are only able to process circa 3-5 transactions per second. Therefore the required transactions capacity has to increase a significant amount in order to counter this challenge regarding a proper implementation of the metering case study.

Another challenge arises with respect to privacy due to the implementation of a fully Blockchain operated electrical energy market. Because of the transparency of the ledger of the Blockchain trading infrastructure could it be possible to deduce the information about closed electrical energy transactions. This would affect the privacy of consumers, electrical energy production companies and energy suppliers within the electrical power system. For example, it could be possible to deduce consumption patterns of specific consumers or the exposure of company specific details about transactions such as the quantity and price of bought or sold electrical energy.

Another challenge which have to be faced regarding the implementation of the metering case study stems from the fact that the energy supplier is still responsible for the balance of load and generation of consumers and prosumers in the metering case study. Therefore, a discussion whether or how the prosumer should be penalized by the energy supplier for over producing or over consuming of electrical energy when there is to much electrical energy within the power system for example due to increased solar power on a sunny day.

5.2.3 Applied knowledge case study

This section presents the challenges regarding the implementation of the applied knowledge case study within the electrical power system. Two categories of challenges to counter can be distinguished namely technical challenges with respect to the electrical power system due to the implementation of the case study and challenges specifically linked to the implementation of the applied knowledge case study.

Technical challenges applied knowledge case study

A successful implementation of the applied knowledge case study requires various technical challenge with respect to the electrical power system to be countered. These challenges mainly relate to the inclusion of transmission and distribution losses into the electrical energy pricing.

Similar as in the previous case study the application of the applied knowledge case study involves the installation of smart metering devices within the electrical power system. In section 5.2.2 the challenges to overcome with respect to the smart metering devices are explained.

The largest technical challenges to counter regarding the implementation of the applied knowledge case study are related to the inclusion of transmission and distribution losses in the electrical energy rates. The main technical challenges which apply to the inclusion of transmission and distribution losses in the electrical energy rates are measuring of the transmission and distribution losses and under / overpricing of transmission and distribution losses.

Basically there are two ways to include the transmission and distribution losses into the electrical energy rates. The first method is to establish a complete map of the transmission and distribution grid including specific details of the transmission and distribution lines, details about the installed conductors, transformers etc. With this map the expected transmission losses and distribution losses of a specific transaction between two parties could be calculated.

However, first of all gathering of all this information would be quiet unpractical and secondly it would require constant updates of the changes within the electrical power system affecting the transmission and distribution losses because it would affect the electrical energy pricing directly. Altogether this would create a quite unpractical and unworkable situation.

The second method would be to install smart metering devices at various points within the transmission and distribution grid of the electrical power system. By measuring the transmission and distribution losses for specific

The second method would be to divide the distribution and transmission grid of the electrical power system into several segments. By installing smart metering devices at these segments of the distribution and transmission grid the occurred transmission and distribution losses could be measured over these segments. For a specific transaction the required segments could be determined and the distribution and transmission losses could be calculated. This method would be more practical opposed to the previous one however it would require extra communication of the smart metering devices with the decentralized computing platform causing the necessity of allocation of extra computational power of the decentralized computing platform.

Another challenge regarding the inclusion of transmission and distribution losses in the electrical energy rates is the under and overpricing of the losses. In the electrical power system the electrical energy flows in inverse proportion to the electrical resistance of the transmission grid and distribution grid. In the current electrical power system the electrical energy can not be routed over specific transmission or distribution lines. Therefore, the calculated transmission and distribution losses could deviate from the actual occurred losses of a specific transaction.

Either this could lead to overpricing of the transmission and distribution losses if the actual losses due to transmission and distribution are smaller than the calculated losses or this could lead to under pricing if the actual losses due to transmission and distribution are larger than calculated.

Challenges specifically linked to the applied knowledge case study

There are also several challenges to overcome which are specifically linked to the implementation of the applied knowledge case study. The main challenges regarding the implementation of the applied knowledge case study are related to the consequences of the elimination of the energy supplier.

The elimination of the energy supplier arises from the introduction of smart metering devices acting as automated agents which could establish electrical energy transactions for the consumers. However, the introduction of the automated agents leads to a large challenge to overcome regarding the required transaction capacity of the peer to peer trading infrastructure. In the Netherlands there are circa 8 million consumers who are interconnected with the electrical power system.

Due to the introduction of smart metering devices acting as automated agents on behalf of the consumers there will be a significant increase of participants on the Blockchain operated electrical energy market opposed to previous situations where the energy suppliers would buy electrical energy for the consumers. If one would assume transaction intervals of 15 minutes, such as in the previous case study, the required transaction capacity would have to be equal to circa 9000 transactions per second whereas the current transaction capacity of current Blockchains such as Bitcoin and Ethereum amounts circa 3-5 transactions per second. Therefore, the current transaction capacity of the Blockchain has to increase majorly in order to be guarantee a successful implementation of the applied knowledge case study.

Another challenge which stems from the elimination of the energy supplier is the responsibility of consumers / prosumers for their balance of consumption and generation of electrical energy. Whereas in the current electrical power system the responsibility for the balance between load and generation of consumers is carried by the energy suppliers. Due to the implementation of the applied knowledge case study consumers and prosumers will bear their own responsibility for their balance between load and generation.

First of all, this requires the operation of the automated agents to be sufficiently fault proof since consumers and prosumers rely heavenly on the operation of these automated agents. Besides that the discussion arises when there is an imbalance between load and generation whether or to what extent consumers / prosumers should be penalized by the transmission system operator.

A different challenge which have to be faced results from the introduction of smart metering devices acting as automated agents. Because of the increased number of transactions the transmission system operator would require a significant amount of processing power in order to process and analyze the data required for the operation of the balancing mechanism of the electrical power system.

5.2.4 Control case study

This section discusses the challenges to counter for a successful implementation of the control case study within the electrical power system. These challenges can be categorized in technical challenges with respect to the electrical power system due to the implementation of the control case study and challenges specifically linked to the implementation of the control case study.

Technical challenges control case study

In order to successfully implement the control case study within the electrical power system several technical challenges have to be countered. These technical challenges with respect to the electrical power system mainly relate to the control of electrical power flows as part of the control case study, the securitization of smart metering devices regarding the implementation of dynamic load shedding.

The implementation of the control of power flows within the electrical power system requires several challenges to be countered. An active distribution network could be created by implementing the control of power flows within the electrical power system. The control of power flows within the electrical power system could be achieved by segmenting the electrical grid, consisting out of the transmission grid and distribution grid, into multiple cells.

These cells within the electrical power system represent a small segment of the electrical grid where a balance between load and generation of electrical power have to be held. These cells consist out of hardware such as smart metering devices, power electronic devices and software which executes control within the specific cell and is employed via the decentralized computing platform of the Blockchain.

For a specific electrical energy transaction between two peers within the electrical power system the electrical energy would be routed from the cell of the source to the cell of the target consumer across the intermediary cells throughout the electrical power system. The route of the electrical energy from generation to consumer should be determined based on available distribution and transmission capacity, transportation cost and cost of the transmission and distribution equipment.

In order to determine the route of the electrical energy the cells will communicate with the decentralized computing platform. With the application of control software via the decentralized computing platform the most optimal route could be determined and control could be enforced in the case of contingencies, outages or power imbalances.

The main technical challenges which are imposed by the control of power flows within the electrical power system relate to the increasing complexity, the increased amount of required computational and transaction capacity of the Blockchain and the cost of the structural changes to the electrical power system.

A decision has to be made over the trade off between the additional complexity of the amount of cells within the electrical power system and the beneficial impact of controlling the power flows to a certain extent. If the electrical power system is divided into more cells complexity will increase with respect to the operation of the control of the electrical power system, structural changes with respect to the electrical power system and the required processing capacity of the Blockchain.

Another challenge has to be countered with respect to the structural changes with respect to the electrical power system and the occurred cost of the installment of these devices throughout the electrical grid. In order to implement the control of power flows extra devices have to be installed depending on the number of cells throughout the electrical grid such as smart metering devices and electrical energy routing devices.

The required transaction capacity of the Blockchain already forms a large challenge. However, due to the implementation of the control of power flows each cell in the electrical power system has to communicate with the decentralized platform. Therefore the required transaction capacity of the Blockchain has to increase a significant amount to facilitate the implementation of control of power flows within the electrical power system.

Besides the required transaction capacity the computational power has to be increased as well due to the implementation of control of power flows. In order to operate the control mechanism and determine the optimal route of the electrical energy the required computational capacity of the decentralized computing platform has to be increased significantly.

Another challenge have to be faced regarding the operation of power flow routing devices and the communication of the devices with the decentralized computing platform. The devices should operate properly and no significant delays should occur in the switching of the devices nor the communication with the decentralized computing platform. Otherwise, this might lead to unintentionally overloading lines within the transmission grid or distribution grid if delays occur between information exchange with respect to the operation of the control mechanism and the actual loading of the lines.

In order to implement dynamic load shedding correctly an important challenge to counter is the secruitization of the smart metering devices. Similar to the previous case studies such as the metering case study and applied knowledge case study the securitization of the smart metering devices should be adequately secure.

However, in the control case study the transmission system operator has the ability to apply dynamic load shedding through the smart metering infrastructure therefore it is highly important that the on the one hand the communication between the smart metering devices and the transmission system operator is properly secured and on the other hand the communication between the smart metering devices and the appliances is adequately secured.

The securitization of communication protocols of current smart metering devices is not properly applied. This should be solved in order to successfully apply dynamic load shedding. Otherwise it might be possible for adversaries to attack the smart metering devices on larger scale in order to create a significant power imbalance. For example, shutting down a whole city which could have a major impact on the stability of the entire electrical power system.

Challenges specifically linked to the control case study

In order to successfully implement the control case study within the electrical power system several challenges have to be countered. These challenges are not specifically linked to the implementation of the control case study. However, these challenges are similar to the discussed challenges in the previous case studies.

5.3 Potential solutions for the various challenges

This section is intended to provide an overview of the various challenges per case study which have been discussed in the previous sections of this chapter and to discuss possible solutions for the various challenges which have to be countered in order to implement the Blockchain and the case studies within the electrical power system.

As discussed there are mainly three categories of challenges per case study: the challenges which relate specifically to the working principles behind the Blockchain, technical challenges with respect to the electrical power system due to the implementation of the specific case study and challenges specifically linked to the implementation of the specific case study.

The proposed case studies in the consecutive order of the market case study, metering case study, applied knowledge case study and control case study provide additional functionalities with respect to the electrical power system compared to its predecessor. As the case studies build up on each other in provided functionality the complexity increases and the various challenges to counter for a successful implementation of the specific case studies build up as well.

In figure 5.1 an overview is presented of the various challenges per category with respect to the implementation of the specific case study within the electrical power system.

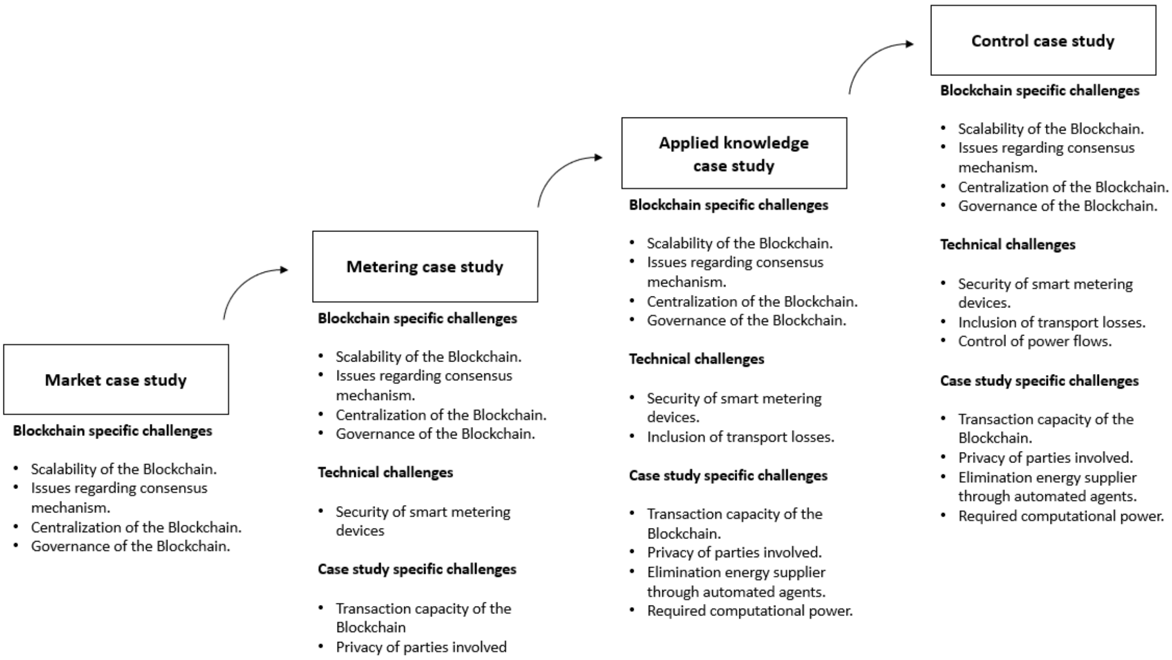


Figure 5.1: Overview of the various challenges per case study

As can be seen in the figure that all the challenges which were apparent in the previous case study also apply on the consecutive case study. As shown in the figure there are large challenges which are specifically attributable to the Blockchain such as the scalability of the Blockchain and issues regarding the consensus mechanism such as the efficiency of the proof of work protocol.

As displayed in figure 5.1 there are several technical challenges as well regarding the implementation of the case studies. The security of the smart metering devices is an important challenge to counter which is introduced in the implementation of the metering case study. The under and overpricing of transmission and distribution losses is introduced in the implementation of the applied knowledge case study. The last substantial technical challenge is the control of power flows which have to be counter for a successful implementation of the control case study.

As shown in figure 5.1 the largest challenges which are specifically linked to the implementation of the case studies involve the required transaction capacity per case study, computational power and the elimination of the energy supplier through the introduction of the automated agents.

Scalability of the Blockchain is by far one of the largest challenges which have to be countered. Currently each node participating within the Blockchain has to process each transaction / blocks in terms of validation and perform each computation on the Blockchain. This greatly compromises the scalability of the Blockchain. As the required transaction capacity increases per consecutive case study this challenge increases in magnitude as well.

There are two different solutions for the scalability issue. Either the size of the blocks of the Blockchain could be increased which would result in an increased throughput of transactions because of the fact that more transactions could be included in a single block. However, the application of increasing the block size is limited because it will require nodes to store more data which causes centralization within the Blockchain as at some point normal computers would not be able to run a node anymore.

Another concept which could provide a solution to the scalability issues regarding the Blockchain is the implementation of a concept introduced by Vitalik Buterin called sharding. The concept of sharding involves that the nodes which participate within the Blockchain network are divided in multiple sub domains which are defined as shards. Transactions, blocks and computations within the Blockchain network which have to be validated and executed are divided over these shards e.g. divided over a subdivision of nodes within the network of the Blockchain. Therefore, transaction output hence the scalability of the Blockchain could be increased without compromising the security of the Blockchain.

Another large Blockchain specific challenge which has to be countered is the poor energetic efficiency of the proof of work protocol as part of the consensus mechanism. A solution for the poor performance of the proof of work protocol could be found in the replacement of the proof of work protocol by the so called proof of stake protocol. In the proof of stake protocol mining nodes within the Blockchain network will lock up a certain amount of virtual currency of the specific Blockchain. Based on the amount of virtual currency which the mining node has locked up it will receive certain voting rights which could be used in order to vote on the rightful consecutive block in the Blockchain. The mining node will validate the transactions within the proposed blocks in order to make sure that only corrects blocks are supported with their vote otherwise the amount of locked up virtual currency will be lost. If a correct block is appended to the Blockchain the mining node will receive an economic reward based on the amount of virtual currency which has been staked. Opposed to the proof of work protocol the proof of stake protocol does not require the consumption of large amounts of electrical energy.

An important technical challenge to overcome is the securitization of smart metering devices. Currently the securitization of smart metering devices is lacking which could form a substantial threat for the electrical power system in general and a weak link in the implementation of the specific case studies. In the smart metering infrastructure there are two communication layers which should be secured. There is the communication layer with the distribution system operator and the smart metering device and the communication layer between the smart metering device and the appliances in the house. A solution in order to improve the securitization of the smart metering device could be implemented by applying proper encryption protocol over both the communication with the distribution system operator and the house hold appliances. On the other hand a proper authentication protocol should be applied for new smart metering devices and new house hold appliances.

Besides the application of encryption and authentication protocols the protocols should be updates at least within a time frame of 10 years before the securitzation protocols will get outdated.

Chapter 6

Practical application of the case studies

This chapter is intended to discuss the practical application of the case studies within the electrical power system which have been presented in chapter 3 and discussed throughout the entire thesis. The case studies will be discussed in increasing order of the level of adoption of the Blockchain. In section 6.1 the application of the market case study will be discussed. Section 6.2 explains the application of the metering case study within the electrical power system. Section 6.3 is intended to discuss the application of the applied knowledge case study. Section 6.4 is intended to explain the application of the control case study.

6.1 The market case study

The market case study has been proposed in chapter 3. The market case study is the most fundamental adoption of the Blockchain within the electrical power system. The implementation of the market case study provides local peer to peer trading infrastructures besides the wholesale electrical energy market where consumers and prosumers have the ability to buy and sell small amounts of electrical energy. As earlier stated the market case study should be considered as a pilot project and will be the first step of adopting the Blockchain within the electrical power system.

In figure 6.1 an overview of the application of the market case study within the electrical power system has been shown. A local trading infrastructure is implemented within a small subsection of the distribution grid which connects a neighborhood. Prosumers and consumers can trade electrical energy with each other via the established trading infrastructure by the Blockchain. On the one hand prosumers and consumers can trade electrical energy with each other on the other hand electrical energy energy is supplied from the transmission and distribution grid as shown in figure 6.1. As depicted in the figure prosumer A sells excess electrical energy to consumer D and electrical energy is supplied to the other consumer and prosumer via the transmission and distribution grid.

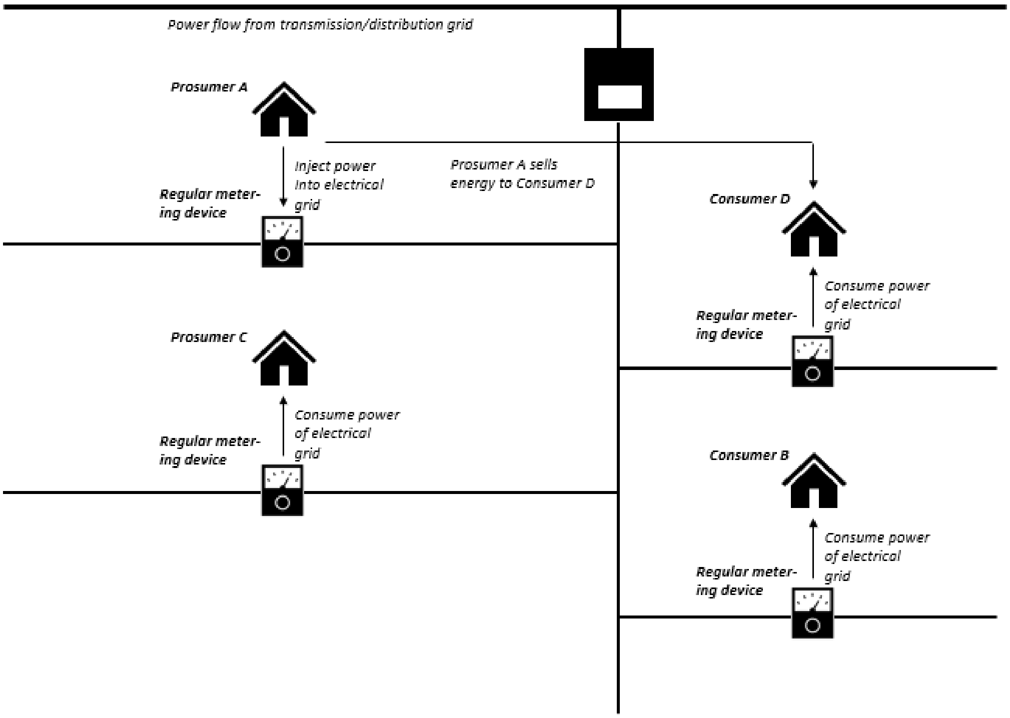


Figure 6.1: Overview of application of the market case study in electrical power system

As could be seen in the figure 6.1 that the houses are connected via regular metering devices this imposes the first challenge for the market case study because the security could not be guaranteed that electrical energy which has been sold via the peer to peer trading infrastructure has actually been delivered. As stated earlier in chapter 3 this problem is classified as the energy double spending problem. The second challenge is imposed by the incompatibility of the metering devices since electrical energy bought via the Blockchain operated trading infrastructure is not distinguishable from electrical energy delivered by the energy supplier.

Therefore, it would be logical and form part of the solution that energy supplier would play a role in developing these local trading infrastructures because on the one hand they could ensure some security to these Blockchain operated trading infrastructures by comparing the bought and sold electrical energy with other energy suppliers. On the other hand they could settle the consumed / bought electrical energy from the peer to peer trading infrastructure with the supplied electrical energy by themselves.

6.2 Metering case study

The metering case study has been proposed and discussed in chapter 3. The metering case study is based on an enhanced level of adoption of the Blockchain and offers simple functionalities with respect to the electrical power system. By addition of computational capacity to the Blockchain a decentralized computing platform has been created. The metering case study involves using these computational capabilities combined with the smart metering infrastructure installed throughout the electrical power system to ensure a higher level of security and integrity. Therefore, the metering case study should be considered as the first practical application of the Blockchain within the electrical power system.

In figure 6.2 an overview of application of the metering case study has been shown. In the metering case study the entire electrical energy market is operated via the Blockchain. Parties involved with the electrical energy market and smart metering devices within the electrical power system exchange information with the decentralized computing platform in order to establish maximum security by eliminating the energy double spending problem.

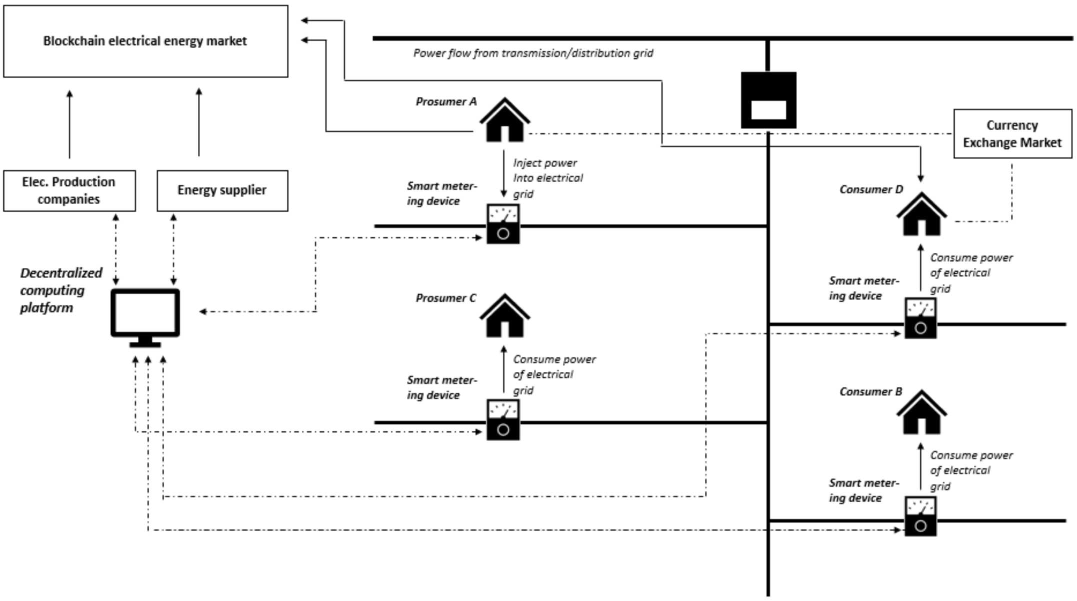


Figure 6.2: Overview of application of the metering case study in electrical power system

As shown in the figure 6.2 prosumer A sells electrical energy to consumer D via the wholesale market which operates via the Blockchain. Consumers and prosumers have the ability to buy and sell electrical energy via the electrical energy market. In essence there would be no necessity for the role of the energy supplier however it would be unlikely that consumers want to bear the responsibility of maintaining the balancce between load and generation. Therefore, in the application of the metering case study the energy supplier is still present.

6.3 The applied knowledge case study

The applied knowledge case study has been proposed in chapter 3. The applied knowledge case study is based on an enhanced level of adoption of the Blockchain. Similar to the metering case study computational capacity has been added to the Blockchain in order to establish a decentralized computing platform in addition to the trading infrastructure.

The application of the applied knowledge case study involves the utilization of this decentralized computing platform in order to gain knowledge about the electrical power system and provide advanced functionalities and features for the electrical power system such as the inclusion of distribution and transmission cost in electrical energy pricing, elimination of the role of the energy supplier and more accurate demand side forecasting.

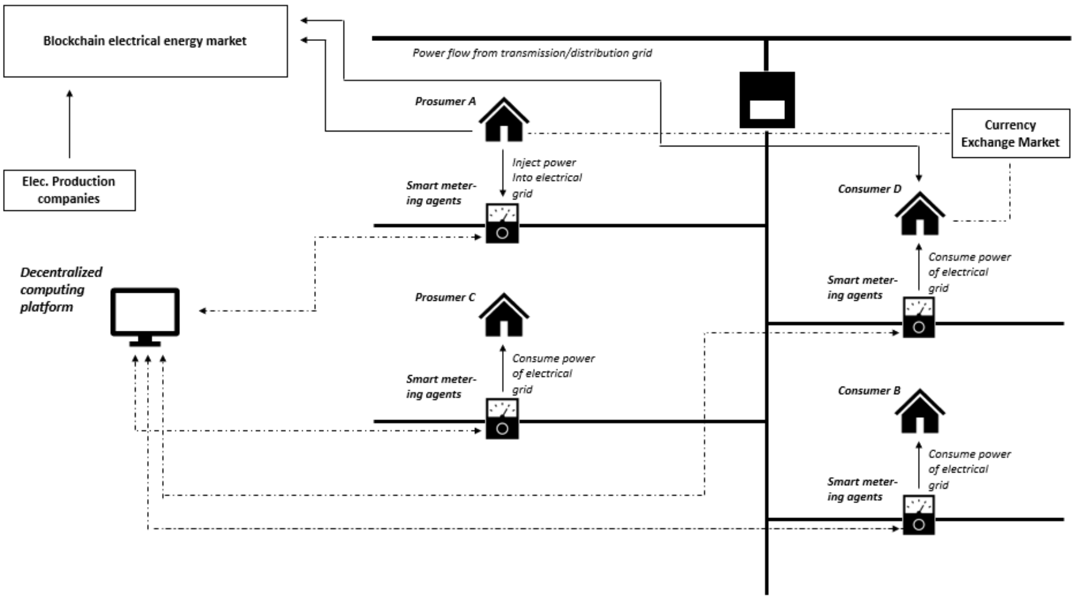


Figure 6.3: Overview of application of the applied knowledge case study in electrical power system

In figure 6.3 an overview of the applied knowledge case study has been presented. As shown in the figure consumers and prosumers directly buy and sell electrical energy on the wholesale market via their smart metering devices acting as agents. Because these smart metering agents buy and sell electrical energy autonomously the role of the energy supplier has been eliminated within the electrical power system.

As could be seen in figure 6.3 is that the applied knowledge case study involves the installation of metering devices within the electrical power system. These installed metering devices combined with the smart metering agents communicate with the decentralized computing platform in order to provide data for advanced features for the electrical power system such as the inclusion of transmission and distribution losses and cost in the electrical energy pricing. And the provision of data for the transmission system operator in order to be able to operate their balancing mechanism more dynamically and accurately.

In figure 6.4 an simplified example of the electrical grid has been shown in order to explain how the cost of transmission and distribution of electrical energy is included into the electrical energy rates. In the figure there are two transactions displayed one transaction between an electrical energy production company and prosumer A and one transaction between prosumer C and consumer B.

As could be seen in the figure the transactions are established between smart metering agents of the parties involved via the Blockchain market. The cost of transmission and distribution of electrical energy is determined based on two elements. First, the actual transmission and distribution cost which occurs through the losses of the transportation of electrical energy through the transmission and distribution grid. Second, the incurred cost of the usage of the infrastructure of the electrical power system such as cost occurred of replacement due to impairment of substations, cables, overhead lines etc.

Based on the specific transaction the decentralized computing platform will calculate the incurred losses of the trajectory of the specific transaction with the data received of the metering devices installed within the electrical power system. The cost of impairments of the electrical power system is calculated based on the trajectory for the usage of the transmission grid and calculated as a constant price per kwh for the usage of the distribution grid. In order to calculate the cost of usage of the distribution grid based on the trajectory of the transaction would be unfeasible because it would require that each line and cable in the distribution grid has to be know and changes have to be updated.

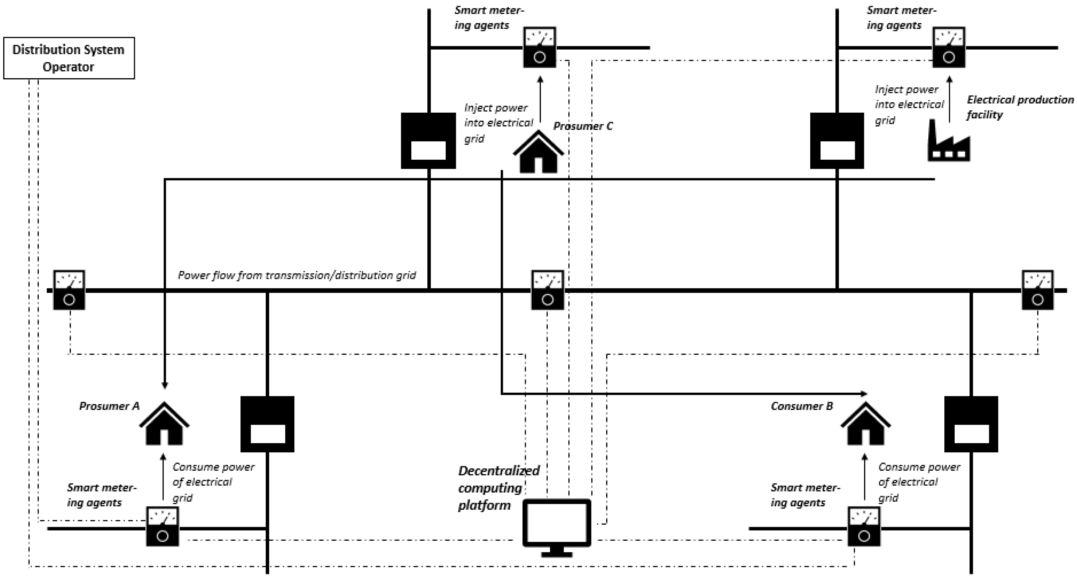
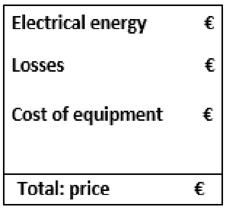


Figure 6.4: Overview of application of the applied knowledge case study in electrical power system

In figure 6.5 there is an simplistic overview of a electrical energy bill.



Electrical energy	€
Losses	€
Cost of equipment	€
Total: price	€

Figure 6.5: Overview Electrical Energy Bill

6.4 Control case study

The control case study has been presented and discussed in chapter 3. Similar to the metering case study and applied knowledge case study the control case is based on an enhanced level of adoption of the Blokchain. Computational capacity is added to the trading infrastructure of the Blockchain in order to create a decentralized computing platform. The control case study involves the application of the decentralized computing platform combined with smart metering infrastructure in order to offer highly sophisticated functions with respect to the electrical power system.

Similar to the previous discussed case study the control case study offers advanced functionalities such as inclusion of transmission and distribution cost and more accurate demand side forecasting. However, in addition to the control case study offers highly sophisticated features such as dynamic load shedding and primarily the ability to control power flows within the electrical power system.

In figure 6.6 an overview of the application of the control case study has been presented. Similar in setup to the applied knowledge case study where prosumers and consumers buy and sell electrical energy via smart metering devices which act as automated agents. The decentralized computing platform is coupled to the smart metering agents combined with power electronic converters installed throughout the electrical power system in order to perform dynamic load shedding and to control the power flows within the electrical power system.

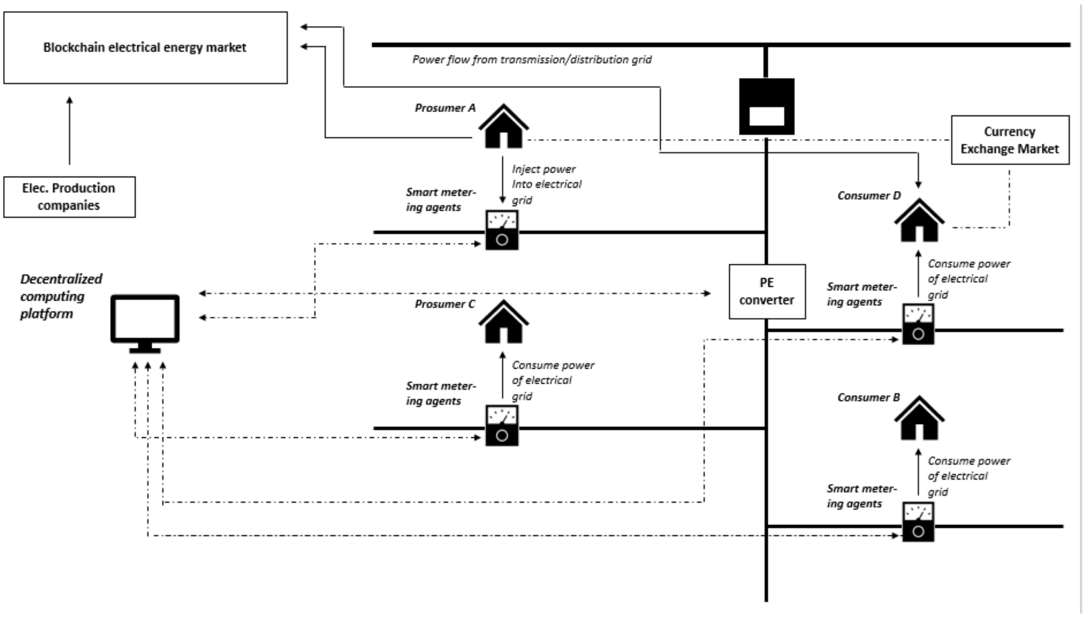


Figure 6.6: Overview of the application of the control case study within the electrical power system

In figure 6.7 a electrical energy transaction has been displayed between a electrical energy production company and a prosumer. The electrical energy is routed through the distribution grid and transmission grid from the electrical power production company to the prosumer. The routing of the electrical energy is performed by coupling installed power electronic converters throughout the electrical power system with the decentralized computing platform. Based on the trajectory of the specific transaction the computing platform will control the power electronic converters in order to determine the power flow. There is a trade of between practicality and decreasing border utility between the control of the power flows within the electrical power system and the number of power electronic converters which should be required in order to so.

In order to fully control all power flows within the electrical power system there should be a power electronic converter installed at each connection of a load. However, it will be more feasible to be able to control power flows on local level within the distribution grid such as being able to control the power flows to a specific neighborhood.

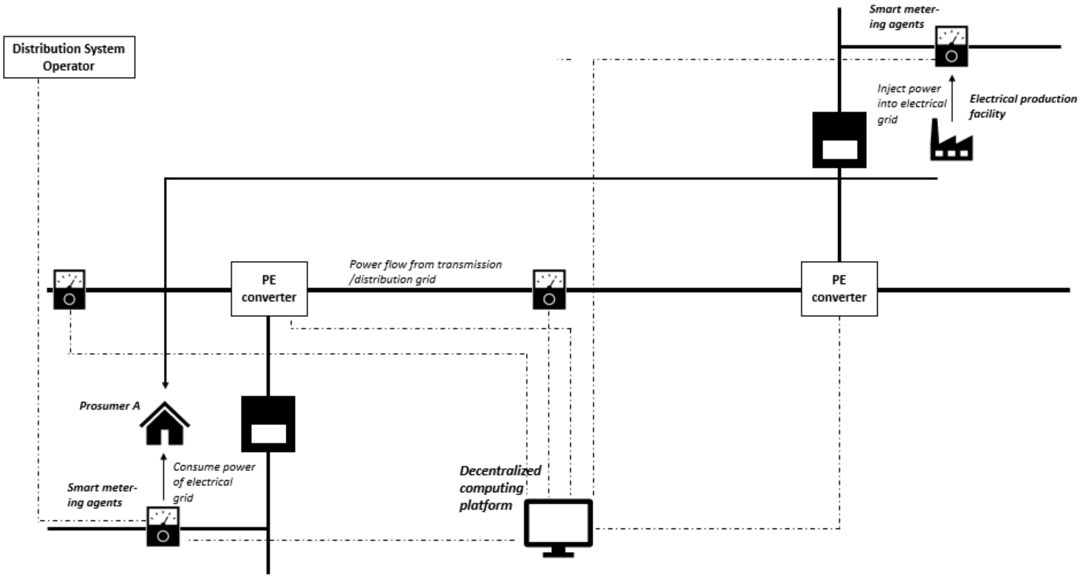


Figure 6.7: Overview of the application of the control case study within the electrical power system

Chapter 7

Conclusion and discussion

This chapter is intended to discuss the conclusions of the performed research. In section 7.1 the results of the research will be presented and a comparison will be made with the research goals. Section 7.2 discusses the results of the master thesis.

7.1 Conclusions

The main goal of this thesis was to identify the opportunities, advantages and challenges of applying the Blockchain to smart grids. The main goal of the thesis was split up into four research objectives. The four research objectives aimed to determine what the Blockchain is and how it operates, where in the smart grid the Blockchain could be applied, what the advantages are of these applications of the Blockchain to smart grids and to identify the challenges for applying the Blockchain to smart grids.

First, in chapter 2 the Blockchain and the operation of the Blockchain have been explained to the reader. The Blockchain has been clearly defined as a collective of technologies which can be described as a database, which is distributed among a peer to peer network, combined with securitization elements relying on multiple cryptographic technologies. The most important technologies which establish the Blockchain are distributed ledger technology, various cryptographic technologies and the consensus mechanism.

At the beginning of the chapter an overview of the Blockchain has been presented and the operation of the Blockchain has been explained. During the following subsections of the chapter various elements and technologies of the Blockchain have been explained in more technical detail such as the characteristics and working principles of the peer to peer network, public and private key cryptography, how transactions in the Blockchain are constructed and the consensus mechanism.

Second, in chapter 3 the opportunities were identified where the Blockchain could be applied in the existing electrical power system. At the start of the chapter different aspects about the electrical power system have been explained and an overview has been presented of the various parties acting within the existing electrical power system and their functions.

After the identification of the potential area for application of the Blockchain into the electrical power system the case studies have been defined. In order to study the application of the Blockchain a classification has been made based on level of adoption of the Blockchain in the different case studies and potential functionality which could be provided to the electrical power system. Based on these definitions four case studies has been proposed: the market case study, the metering case study, applied knowledge case study and control case study.

These case studies are based on different levels of adoption of the Blockchain and the functionality which could be provided to the electrical power system ranges from offering basic functionality to highly advanced functionalities. The market case study involves the application of a local peer to peer trading structure via the Blockchain. The metering case study builds on the market case study, by addition of computational power to the Blockchain a decentralized computing platform is established which makes it suitable to establish a fully Blockchain operated market. The applied knowledge case study offers advanced functionalities to the electrical power system such as inclusion of transmission and distribution cost besides a fully Blockchain operated market. The control case study involves highly advanced features through application of the Blockchain such as the control of power flows within the electrical power system.

Third, in chapter 4 the advantages to the electrical power system were explained of applying the Blockchain as proposed in the various case studies. At the beginning of the chapter the advantages of applying the Blockchain are discussed which are specifically attributable to the characteristics of the Blockchain. The major advantages being increased resilience, decentralization of trust and increased security.

In the following subsections of the chapter the advantages of the implementation of the various case studies are considered. The market case study should be considered as a initial step in the adoption of the Blockchain which primarily offers a local peer to peer trading infrastructure in order to integrate the increasing amount of prosumers in the electrical power system. The implementation of the metering case study is the first practical application of the Blockchain within the electrical power system. It offers the required secrurity to be employed within the electrical power system and all advantages specifically linked to the characteristics of the Blockchain are applicable for this case study. The applied knowledge case study is the first application of the Blockchain where the potential functionalities of the decentralized computing platform are employed. It involves advanced features to the electrical power system such as the inclusion of transmission and distribution cost into the electrical energy pricing. The control case study should be regarded as the most advanced adoption of the Blockchain. It uses the full potential of the decentralized computing platform and offers highly sophisticated features to the electrical power system such as control of power flows within the electrical power system, dynamic load shedding.

Fourth, the challenges of applying the Blockchain to the electrical power system were discussed in chapter 5. At the beginning of the chapter the challenges specifically linked to the characteristics have been discussed. The challenges, based on several themes, have been analyzed such as issues regarding the consensus mechanism, factors causing centralization within the Blockchain and issues regarding the peer to peer network of the Blockchain.

Throughout the continuation of the chapter for each of the case studies the technical challenges to the electrical power system and challenges specifically linked to the case study are analyzed and discussed. As stated earlier the market case study is the initial step in the adoption of the Blockchain and it faces issues regarding the security of the trading infrastructure due existence of the double energy spending problem. The metering case study faces challenges regarding the securitization of the smart metering devices, scalability of the Blockchain in order to ensure proper operation of a Blockchain energy market. The largest challenges which are applicable to the applied knowledge case study are pricing of the cost of the transmission and distribution of electrical energy, the scalability issues regarding the introduction of smart metering devices acting as automated agents and the responsibility for consumers and prosumers due to the elimination of the energy supplier.

In order to implement the control case study the largest challenges to counter are related to the control of the power flows within the electrical power system which leads to challenges regarding scalability issues of the required communication with the decentralized computing platform. At the end of the chapter the challenges per case study are summarized in a figure which shows how the Blockchain specific challenges, technical challenges and case study specific challenges build upon each other per case study.

Last, the practical application of the Blockchain to the electrical power system of the different case studies have been discussed in chapter 6. An explation is given to the reader how the case studies could be implemented within the electrical power system and what the role will be of different parties currently involved within the future electrical power system.

7.2 Discussion

During the research of this master thesis Blockchain as a technology has gained momentum mainly through the evolving industry of crypto currencies, the rise of Bitcoin etc. New concepts which employ the Blockchain are funded due to the existence of excessive liquidity in the crypto currency market. Currently the outlook on the Blockchain as a technology is too optimistic and the expectations of the value of the technology are too high, similar to the outlook and expectations of at the beginning of the internet.

This thesis provides a clear view of the potential advantages of the application of the Blockchain to the electrical power system however it also presents a critical view on the challenges which have to be faced in order to guarantee a successful application within the electrical power system. The latter being highly important due to the exaggerated outlook on the Blockchain.

The application of the Blockchain within the electrical power system has certainly potential advantages. These advantages stem from the advantages attributable to the characteristics of the Blockchain and the potential advantages of the additional functionality it could provide to the electrical power system. These potential advantages differ per case study as adoption of the Blockchain and functionality evolves and builds onto the previous case study. The first realization of the advantages specifically linked to the characteristics of the Blockchain occurs after implementation of the metering case study. The implementation of the metering case study will be extremely valuable to the electrical power system in order to manage the increasing group of prosumers within the electrical power system. The advantages which are derived from functionalities are derived after the implementation of the applied knowledge case study and control case study. Whereas the major advantages derived from functionality are the inclusion of transmission and distribution cost and the control of power flows for the applied knowledge case study and control case study.

However, in order to successfully implement the Blockchain within the electrical power system significant challenges have to be countered as well. The main challenges for the application of the Blockchain are related to challenges specifically linked to the Blockchain and (technical) challenges related to the implementation of the actual case study. Whereas, factors causing centralization or the excessive energy consuming of the consensus mechanism are large challenges to counter scalability forms the largest challenge to counter for the application of the Blockchain within the electrical power system. At current moment the Blockchain is not scalable resulting in a limited transaction throughput capacity. This challenge only increases in magnitude as the required transaction throughput increases as the case studies evolve in adoption of the Blockchain and functionality. Especially after implementation of the applied knowledge case study which introduces the smart metering devices acting as automated agents.

In chapter 6 has been described how the Blockchain could be applied to the electrical power system. For the integration of the Blockchain in to the electrical power system it would certainly be logical that the market case study should be the initial step in adopting the Blockchain. Larger energy suppliers definitely could play a role in establishing local peer to peer trading infrastructures via the Blockchain. As the Blockchain evolves smart metering devices are coupled to the decentralized computing platform in order to make it suitable for employment for the total market as defined as the metering case study. However, even the implementation of the metering case study would require a significant evolution of the Blockchain as technology and a likely time frame for the implementation would be at the earliest in 5 years. On the further horizon there is the implementation of the applied knowledge case study and control case study. Whereas, the elimination of the energy suppliers by automated agents and inclusion of transmission, distribution cost into electrical energy pricing and control of power flow would require significant structural changes within the electrical power system and challenges to be countered. A likely time frame for the implementation of the applied knowledge case study and control case study would 7-10 years.

Bibliography

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[2] A. Smith, “Desperately seeking satoshi; from nowhere, bitcoin is now worth billions. where did it come from?” *Sunday Times*, 2014.

[3] A. M. Antonopoulos, “Mastering bitcoins,” 2014.

[4] S. William. (2017) Record 121 bln crypto market cap comes as bitcoin share dwindles. [Online]. Available: https://cointelegraph.com/news/record-121-bln-crypto-market-cap-comes-as-bitcoin-share-dwindles

[5] H. Kevin. (2017) These exchanges are now trading bitcoin cash. [Online]. Available: https://news.bitcoin.com/exchanges-trading-bitcoin-cash

[6] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond bitcoin,” *Applied Innovation*, vol. 2, pp. 6–14, 2016.

[7] V. Buterin *et al.*, “Ethereum white paper,” 2013.

[8] K. Rabah, “Theory and implementation of elliptic curve cryptography,” *Journal of Applied Sciences(Pakistan)*, vol. 5, no. 4, pp. 604–633, 2005.

[9] A. I. Badev and M. Chen, “Bitcoin: Technical background and data analysis,” 2014.

[10] R. Naik and N. T. Courtois, “Optimising the sha256 hashing algorithm for faster and more efficient bitcoin mining,” 2013.

[11] D. Meijer, “Consequences of the implementation of blockchain technology,” 2017.

[12] B. Barak, “The complexity of public-key cryptography,” in *Tutorials on the Foundations of Cryptography.* Springer, 2017, pp. 45–77.

[13] S. Peng, “Bitcoin: Cryptography, economics, and the future,” 2013.

[14] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[15] D. Wang, “Secure implementation of ecdsa signature in bitcoin,” *Information Security at University College of Longon*, 2014.

[16] B. Jana and J. Poray, “A performance analysis on elliptic curve cryptography in network security,” in *Computer, Electrical & Communication Engineering (ICCECE), 2016 International Conference on.* IEEE, 2016, pp. 1–7.

[17] J. A. Kroll, I. C. Davey, and E. W. Felten, “The economics of bitcoin mining, or bitcoin in the presence of adversaries,” in *Proceedings of WEIS*, vol. 2013, 2013.

[18] J. Bergquist, "Blockchain technology and smart contracts: Privacy-preserving tools," 2017.

[19] CBS, "Electriciteit in nederland," 2015.

[20] I. E. Bureau, "Stroomnet onder hoogspanning: staat gebaat bij kruisparticipaties netbedrijven," 2014.

[21] P. F. Monti A, "Electrical power systems," 2015.

[22] F. Economics, "Scenarios for the dutch electricity supply system," 2015.

[23] L. v. d. S. Pieter Schavemaker, "Electric power system essentials," 2017.

[24] B. Gombert, "Dynamic electricity management flexibility of demand in the dutch electricity market," 2014.