Blockchain based Peer-to-Peer Energy Trading using IoT devices

by

Komal Khan

Submitted to the Department of Electrical Engineering, Electronics,
Computers and Systems
in partial fulfillment of the requirements for the degree of
Erasmus Mundus Master Course in Sustainable Transportation and
Electrical Power Systems
at the
UNIVERSIDAD DE OVIEDO
August 2019

Author . . . .

Certified by . . . .

Dr. Pablo Arboleya
Associate Professor
Thesis Supervisor

Certified by . . . .

Dr. Islam ElSayed (Co-Supervisor)
Postdoctoral Researcher
Thesis Supervisor

Blockchain based Peer-to-Peer Energy Trading using IoT devices

by

Komal Khan

Submitted to the Department of Electrical Engineering, Electronics, Computers and Systems
on August 31, 2019, in partial fulfillment of the
requirements for the degree of
Erasmus Mundus Master Course in Sustainable Transportation and Electrical Power Systems

Abstract

Increased penetration of Renewable Energy Sources(RES) and ever expanding global energy demands push forward the need of efficient utilization of RES by incorporating the prosumers (who are able to inject produced renewable energy) into the energy infrastructure. Moreover, there is emerging demand of the prosumers to participate in the electricity market and monetise their contributions. In order to facilitate these demands, the traditional centralised architectures are no longer viable therefore a decentralised transactive energy system enabling peer to peer energy trading, should be adopted. In this context, Blockchain based decentralised ledger technology emerges as the most viable solution which offers peer to peer energy trading platform providing a unique distributed local energy market model(LEM) for beneficial energy exchanges among participants which represents evolution for future smart grids.

This thesis provides comprehensive review of the fundamental characteristics of the blockchain technology and its promising solutions for the energy industry. P2P energy trading, one of the use case of blockchain in energy sector has been focused and explored by thoroughly reviewing various initiatives, research and pilot projects that are currently working in that area. Moreover potential challenges pertaining to this blockchain based application are also evaluated. Based on the extensive research and literature review, a simple model of blockchain based peer to peer energy trade using IoT devices has been developed. Hence, this thesis provides all the necessary technical details and steps required to build the simple model of blockchain application for energy transactions.

Thesis Supervisor: Dr. Pablo Arboleya
Title: Associate Professor

Thesis Supervisor: Dr. Islam ElSayed (Co-Supervisor)

Title: Postdoctoral Researcher

Acknowledgments

First and foremost I am highly grateful to Almighty Allah for never letting my efforts go unrewarded and for the successful completion of this project. I am deeply obliged to my advisor Dr. Pablo Arboleya, for his unwavering support to me throughout my thesis with his patience and knowledge whilst allowing me to explore on my own, and at the same time the guidance to recover when my steps faltered. You have been a tremendous mentor and a role model for me, one simply could not wish for a better or friendlier advisor. I would also like to take this opportunity to greatly thank for the most important personality, without whom this project could never have been successful, my co-supervisor Dr. Islam ElSayed for his guidance and support throughout the project, especially his critical analysis on my work and his confidence in me. A big credit goes to him since he directed me in the development of this project and encouraged me to attend various valuable courses which helped me in improving my programming skills and understanding of the subject technicalities.

I would also like to extend my gratitude to all my colleagues who helped me during the process with their valuable suggestions and guidance to be where I am today especially Xavier Dominguez and Prof. Bassam Mohammed. Also worth mentioning here my peers from the STEPS third batch, with whom I've shared an amazing experience and made so many memories over the course of these two years.

My sincere thanks to my friends and all those that in any way contributed or helped me be where I am today especially Imtisal-e-Noor. Last but not at all the least, I am grateful to my family and in particularly my parents for always being the beacons of light that guided me on my journey to this point and for providing me with every kind of support I needed throughout my life.

Dedication

To my parents, for giving me strength and courage to show the best of my abilities, for earning an honest living for me and making me what I am today.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In the last decade, a significant proliferation of renewable energy sources (RES) has been witnessed in the energy production landscape. Around 30% of world electricity production will come from RES by 2022 according to International Energy Agency (IEA) [1]. And it'll further exceed up to 60% in coming 2050 [14]. On the other hand, the electricity demand is suspected to increase by 20% in the following decade due to the increased penetration of EVs, energy storage systems, smart appliances [15]. Although, the rapid growth of RES is a good indication to tackle rising energy demand and to meet targets towards sustainability development and decarbonisation. However, there still lies a requirement of efficient utilization of this renewable energy.

In the pursuit of resolving this issue, Microgrid framework has been introduced as a solution to manage portions of distribution networks where there was both consumption and distributed generation [16]. However microgrids experience stability issues due to the intermittent nature of the renewable energy and offers few or not-existing direct economic benefits to the distributed energy producers [17]. Moreover, centrally controlled energy systems by utility companies and network operators, imposes high costs on the electricity we use. Furthermore, the energy market regulations and the management of energy trading also need some consideration.

In recent years, the advancements in digital and communication technologies have emerged as a revolution which has paved the way towards innovation in almost every field. In the last decade, the introduction of the advanced smart meters and other smart appliances based on the Internet of Things (IoT) gave rise to the concept of smart grid in the power industry, which suggested a better solution to incorporate the distributed energy production and manage demand-supply energy [18]. At the beginning of 2013, after the outstanding success of blockchain 1.0 (Bitcoin cryptocurrency) [19], blockchain 2.0, the second generation emerged with the advanced smart contract technology, which opened an era of automated society. This technology introduced concepts such as Decentralized Applications (Dapps), Decentralized Autonomous Organizations (DAOs) and Decentralized Autonomous Corporations (DACs) [20], which brought disruption in almost every industry and suggested a new paradigm change in the power industry.

Blockchain 2.0 offers the democratisation of existing power systems by introducing a whole new concept of peer-to-peer (P2P) energy trading [21]. This allows the energy producers and consumers so-called "prosumers", to trade electricity locally which reduces electricity transmission losses but also offers optimization of power flow, grid stability improvements, demand-side management and cost-effective utilization of distributed energy [22]. Moreover, P2P trade could be a win-win situation for prosumers and also profitable for typical consumers as the prices are negotiated which may be lower than the ones imposed by the existing electrical markets [18]. A great potential of the blockchain technology can also be seen in other sectors such as in financial business operations where the emergence of bitcoin lead to a very significant position because of its transparent, verified and auditable financial services applicable for the banking and financial institutes. Nonetheless, the notable blockchain-enabled applications in health care, supply chain, asset management, chemical industry and other sectors, prove blockchain to be a promising technology also for the energy sector [23].

The potential of blockchain has been exhibited by the efforts of some proactive electrical companies and startups in the form of pilot projects. Brooklyn Microgrid [24] and Power Ledger [25] are one of the first pilot projects who made it possible for the participants to share energy and earn revenue. More contributions have been made by other prominent companies like Verv [26] which supports its trading platform by their ultra high resolution smart meters, Grid+ [27] which has designed Grid+ agent to provide retail supplier services, and others. There is also a massive research in progress to explore more opportunities hidden behind this field of technology. However, there are still not significant publications detailing the design and implementation of blockchain-based energy applications; and to date, almost all papers related to this field majorly discusses about the market impact, business aspects and a surface knowledge about technical development but do not specify much technical implementation details. In this regard, this thesis provides the road map to understand step by step the blockchain technology, development and implementation of P2P energy trading model based on the Ethereum Blockchain framework.

Undoubtedly, this technology has offered tremendous solutions to the problems associated to current power system network but still faces some technical challenges such as consensus mechanisms, storage and data management, and chain structures, as well as research challenges such as regulation and governance [11]. Nevertheless, blockchain is a scalable platform and also a fast-moving area of research and development because in a short time span, a great advancement and development have been witnessed in this field. Additional research initiatives e.g possible integration of AI, cloud computing and machine learning algorithms with blockchain could help in unlocking the full disruptive potential of this technology which makes it suitable for market reliability and to be deployed at a large scale [13].

1.1 Research goals

A systematic approach will be acquired in this thesis to give full understanding of the blockchain technology and its useful application for peer to peer energy trading in order to meet the current challenges faced by the traditional power systems and the emerging need of transformation towards transactive management infrastructure.

The goal of this thesis is to carryout an in-depth literature review on the blockchain use case in energy sector and apply research methodologies in order to collect enough resources and understanding of the technology, to design and implement a simple basic model of blockchain based P2P energy trading. Once the goal is achieved, it is intended to add more enhancements in it in near future.

All the key knowledge and basic understanding acquired during the development of this model is intended to be included in this thesis.

1.2 Thesis structure

The rest of the thesis is structured as follows:

Chapter 2 describes the prevailing challenges pertaining to the conventional power grids architecture due to the inflation of renewable energy resources. It discusses existing energy trading solutions to meet these challenges.The evolution of smart grids and the need of blockchain technology to enable peer to peer energy transaction, is explained in this chapter.

Chapter 3 introduces blockchain technology providing deep background and conceptual understanding of its characteristics and fundamental principles including structure, hash cryptography, consensus protocols, mining, distributed P2P network. It discusses the two largest blockchains, Bitcoin and Ethereum. Ethereum platform, smart contract technology and decentralised applications are discussed in detail to provide the basic concepts required for building own application. In the last, prevailing challenges to the blockchain are discussed.

Chapter 4 introduces blockchain based transactive energy systems and emphasises on its advantages over traditional centralised architectures. It highlights the main services of the blockchain in energy sector and focuses on its use case of P2P energy trading. Core technologies are explored that can potentially enhance capabilities of blockchain. Notable pilot projects, companies and platforms are also highlighted and discussed. Different surveys, statistics of blockchain energy projects and their lists are also been referenced. In the end, main challenges pertaining to this field are also discussed.

Chapter 5 gives detailed technical information about the implementation of basic P2P energy trading model. Main idea or scenario, hardware and software tools, smart contract development, application development and the interoperation of all of these are illustrated in this chapter.

Chapter 6 concludes the thesis as it provides the discussion over the results achieved and conclusion along with the insights for the future work and developments.

Chapter 2

Energy Trading

2.1 Conventional Power Grids

Electrical power systems have been serving the world energy needs for over a century. These systems have greatly relied upon the large remote power plants which run on conventional sources (fossil fuels, coal, natural gas), high-voltage transmission systems and low-voltage distribution systems to pass on electricity finally to the consumption side i.e. the loads [28]. These conventional power systems have centralised management system which involves a range of actors who manages the electric grid and its operations i.e. controlling and scheduling the electricity production and delivery to the consumer end with provided reliability and low cost electricity package. These actors include power generators, energy supply companies and markets, transmission network and distribution system operators and regulatory bodies. The governance structure of the power systems decides the technical settings of these actors i.e. their roles and responsibilities in the whole supply chain. Therefore, regulatory structures, market rules and policies have great influence on the role of actors. And this characterises most of the electrical power systems around the world [29].

2.2 Rise of RES

However, over the last few years, electric power systems have begun to change mainly due to the actions taken by energy policy makers against rising environmental pollution and energy crisis world wide. The RES directive establishes binding targets for each member state of the RES share in gross final consumption by 2020 [30]. Different agendas and schemes have been introduced to reduce the dependencies from fossil fuel markets [31]. Renewable energy systems are being promoted in the market as many governments around the world have initiated financial support programs to encourage consumers to install renewable energy systems, and incentive based programs are designed to reward renewable energy production [31]. Moreover, a significant decline rate in the prices of renewable-energy equipments have been observed [32]. As a result, an inflation can be seen in the sale and production of RES(as shown in Fig.2-1). A large number of participants are now becoming a part of micro scale renewable energy production, installing variety of RES e.g. top solar panels, fuel cells, batteries, micro turbines, and more from the renewable technology world [32].These participants are termed as prosumers, a combination of producer and consumer due to the fact that they produce energy but still depend on conventional power systems for their major energy needs.

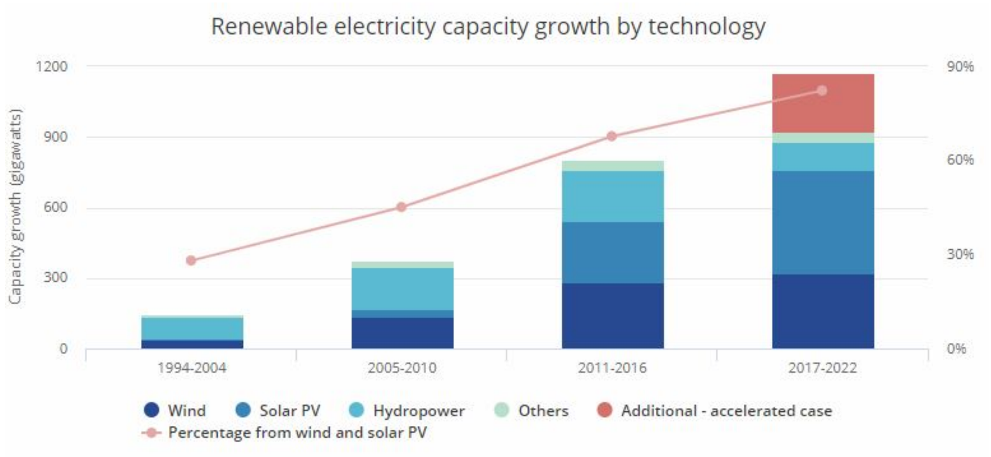


Figure 2-1: Growth rate of Renewable Energy [1]

2.2.1 Challenges of RES integration

In this context, it is expected that in 2022, around 30% of world electricity production will come from RES according to International Energy Agency (IEA) [1]. Although, rising renewable energy production is achieving the agenda of establishing a low-carbon electricity sector, it also challenges the technical settings of the existing electricity regime. Since renewable energy is intermittent in nature as it depends on the weather conditions, season and time of the day. Moreover, it is difficult for the existing grid capacity to withstand the stress of increasing bidirectional variable flows of energy [33]. Moreover, existing governance structure requires enhancements in order to incorporate players known as prosumers into the energy infrastructure. Furthermore, the introduction of EVs, smart devices and digital technology is an obvious sign of energy demands surges which push forward the need of better management of RES. In this regard, main challenges pertaining to the development of the power system infrastructure for integration of RES, are:

1. Centralised management system: system operators control power supply to manage the fluctuating energy demands but now there is addition of fluctuating energy supplies i.e.varying RES which makes the management more complex.

2. Minimal real-time information: Bidirectional communication between system operators and system users is required which means operators need real time information about the grid operations, especially the consumption and generation made by the end users at distribution level, to harness the demand flexibility [34].

3. Conventional long distance one way power transmission: the system is currently vulnerable to bidirectional variable flow of RES which stresses the grid capacity.

4. Governance structure: a revised governance structure and legal framework is required to adjust the changing roles of consumers into prosumers [35].

2.3 Smart Grids

In order to achieve a low carbon electricity system, the power grid infrastructure needs to show compatibility with RES. To meet these challenges, a new generation of power grid concept has been introduced i.e. Smart Grids. Smart grids are the cost effective solution for existing power grids with an upgrade design and operation which promises efficiency and fulfills the supply-demand balancing needs.Smart grid accommodates Internet-of-Things (IoT) devices such as smart meters for advanced metering into the electrical power systems. These devices enable bidirectional communication which provides the dynamic infrastructure for managing the energy demand response [36, 37].

Aggregation of IoT technology with the system allows a real time monitoring of both the generation and consumption, resulting in an intelligent power system that welcomes distributed power generation and new actors i.e. prosumers. Prosumers could sell their produced energy, add flexibility in their energy demands and provide energy balancing services that are beneficial for the RES integration to the power system. Thus, smart grids avenues further developments in the power sector. However, legal frameworks to incentivise such participation and market structures which enable prosumers as active market players, are still under planning phase. In addition, there are some prevailing challenges for smart grids related to its security and privacy [38] due to the introduction of the communication technologies which are prone to cyber attacks.Moreover, cost is another factor which appears when transitioning to smart grids and that stresses upon looking for new possible solutions.

2.4 Blockchain

In the recent years, blockchain emerged as a disruptive information technology and as an industrial revolution, opening a new era of decentralization and democratisation. Blockchain has a potential to address the upfront challenges to power grids. This technology presents several solutions:

1. Grid Resilience: Prosumers could become independent market players to transact energy directly under automated smart contract, independent of third parties [33].

2. Security and Privacy: Blockchain offers distributed ledger system, secured with cryptographic power and decentralized infrastructure to achieve cyber resiliency and secured transactions [39].

3. Cost Reductions: Blockchain based smart contracts provides distributed market coordination which improves transaction costs. economics [39] as compared to local energy market model because of third parties major involvements.

Thus, blockchain technology holds disruptive potential for its application in the energy sector. It offers p2p energy trading platform for useful and efficient integration of RES with grid resulting in more secured, decentralized and resilient power grid.

Chapter 3

Blockchain Technology

3.1 General Overview and History

In 1991, an idea was originated about digital time stamping of the documents to preserve them and resist modification subjected to them. It was the first paper published which introduced different features and concepts like hash cryptography, time stamping services, linking and distributed trust that later formed the basis of Blockchain technology [40]. In 2008, a pseudonym referred as Satoshi Nakamoto published a paper introducing the first Blockchain concept for bitcoin, a peer to peer electronic cash system [19]. This paper introduced a consensus mechanism ”proof of work” for validating transactions and updating on a public ledger. Satoshi Nakamoto, the invertor of the blockchain technology, didn’t use the ”blockchain” term in the paper. However, this term was introduced in the source code of bitcoin in 2016 [41] which later became widely famous as Blockchain.

3.1.1 Structure

Blockchain is a decentralized and distributed digital ledger that records the data or information in encrypted form, in blocks that are linked and secured cryptographically so that the data can’t be modified or forged [42]. It uses a consensus mechanism to validate the data and store it into the ledger. Blockchain is named for its data structure which consists of blocks of data that are chained together using cryptographical hashes. Hash could be assumed as a finger print assigned to each block, this concept will be further discussed in later sections. A block in the blockchain contains a header and a payload. The header includes the information about timestamp, the cryptography hash of current and previous block and other details regarding mining and consensus mechanisms, as shown in Fig. 3-1. While the payload of the block contains the data or transactions stored in it. The first block of the blockchain is known as genesis block, the trail of the records start from this block. Unlike the rest of the blocks, the genesis block doesn't have a hash of the previous block. However, the hash of the genesis block becomes the previous hash of the next block and thus the chain continues.

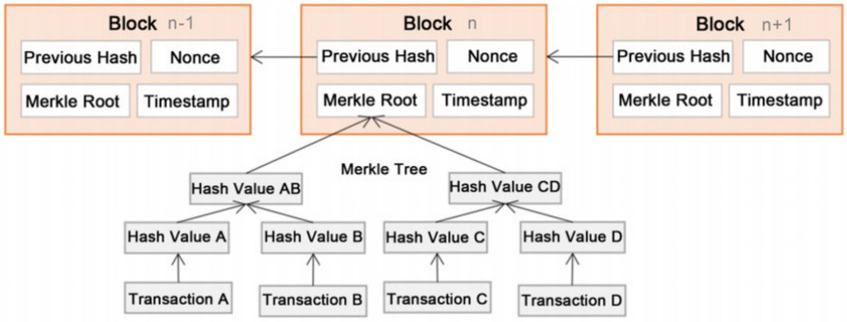


Figure 3-1: Structure of Blockchain [2]

This linking scheme is useful to avoid data tampering as each block confirms the validity of the preceding blocks. Therefore, if any modification is encountered in any block, the following blocks of the chain become invalid. Hashes of all the transactions stored in a block are also hashed and linked together as a part of a Merkel Tree (as shown in Fig.3-1). Merkel tree can be defined as a data structure which takes an input of n number of hashes and produces a single hash representation known as Merkel root, which is specified in the header of the blocks. This mechanism is useful to access and validate any large set of data with simplified verification process which only checks if the hashing of the data is consistent with the hashes of tree without going through entire set of hashes [19].

3.1.2 Properties

Hash Cryptography

A fingerprint is used as robust identifier of a person, hence it is widely used by administrations and forensics departments. The same principal is applied to digital documents. In this regard, the fingerprints for their identification have been evolved and called as SHA256 hashes [3]. The Secure Hash Algorithm (SHA) was first developed by the NIST (American National Institute of Standards and Technology) in association with NSA (American National Security Agency) in May 1993 [3]. As the initial SHA function was cracked/broken with computing power, the algorithm was revised in 1995 and published as SHA-1. It took 7 years to break the SHA-1, hence the NIST developed more complex functions and published the stronger hash algorithm SHA-2 (SHA-224, SHA-256, SHA-384 and SHA-512) which uses longer hashes to make the attack difficult. Then, it was suspected that a brute force attack could crack SHA-2 in the future. Therefore in 2007, SHA-3 hash function was announced and later published in 2012. Currently, blockchain uses SHA256 hash algorithm for encryption of data.

Cryptographical hash algorithms apply hash functions to the input data and produces a unique and fixed length 'fingerprint' string known as Hash. This algorithm works in two phases, first, an input message is expanded and followed by some transformations which are iterated. Secondly, bitwise shifting is applied using some logical operators. Additionally, some other functions are also used for data mixing [3]. The algorithm doesn't only work for text or documents but for any digital data like videos, audios or any executable files. SHA-256 produces a 64-character length hash which is very strong and difficult to attack [3] . Fig.3-2 illustrates the aforementioned algorithm.

There are five certain properties of Hash Algorithm which makes it applicable for encryption purposes in blockchain. They are :

1. One-Way : Hashes are like fingerprints for humans as earlier mentioned. Nevertheless, the appearance of a person can't be derived from his fingerprints.

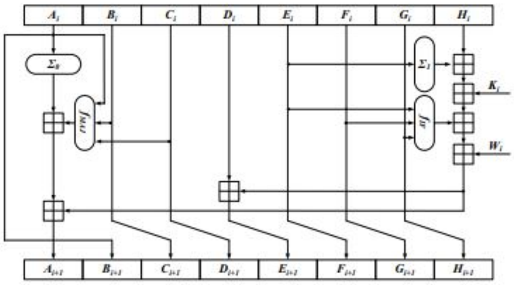


Figure 3-2: SHA-2 [3]

Similarly, a digital document can't be restored or reverse engineered based on its hash.

2. Deterministic : For the same document, when a hash algorithm is applied again, it has to produce the same hash as it did for the first time.

3. Fast Computation : Hash computation needs to be fast to avoid tampering and forging of the document.

4. Avalanche Effect : A minor change in a document completely changes its hash. Functions inside the algorithm are implemented in a fashion that small changes in the input document trigger significant changes, resulting into a completely different hash.

5. Withstand collision : As the amount of digital data is much greater than the different number of variations of a 64 character hash representation, a pigeon hole principal (fit in all the pigeons in given number of holes) can be applied to accommodate this enormous data with hashes available because it is probable to have collisions, i.e. two documents having same hashes may rarely occur. Therefore, the algorithm must have the ability to withstand these collisions.

These properties forms the basic foundations of secure and safe hash cryptography which are highly significant for the blockchain technology.

Immutable Ledger

Ledger is a record book of any type of data, from a small retailer shop to a big government institute. Legders confirm identity, ownership, authority, status, mapping economic and social relationships [43]. Physical actual books when used as ledgers are unreliable and unsafe to data tampering. Some countries have experienced financial crises due to natural disasters, as they lost highly important physical ledgers, which is very troublesome in the cases like property ownership records. For this reason, in the last decades, ledgers have been digitised. The Australian passport ledger system became one of the first digitised and centralised systems in 1970 [44] and other nations followed the trend. Although, the database has made the job quite easy in terms of computation and safety, its reliability depends on the authenticity of the organisation who holds it.

In these days, to add transparency, reliability and security to ledgers, blockchain comes into the power. Blockchain is a digital, distributed and decentralised ledger. In order to understand how it secures the data, a property ledger traditional approach versus a blockchain approach can be taken as an example to expose how blockchain can add protection and make the ledger immutable. Assuming that titles of property owners are stored in the blockchain of a government authority rather than a paper or database. Each time the buy or sale of a house occurs, this transaction is added into a block of the ledger. Now, if a person tries to temper the data of a specific block, it changes its hash which no longer matches with the previous hash field of the next block, thus the cryptographic link will break. Unlike the ledger book, a person can not just change the entry, instead he has to change all the entries following the current one. This is what an immutable nature of blockchain means, because data can not be changed as soon as it is stored inside the block. In this way, government ledgers could be secured be secured by means of blockchain.

On the other hand, in the case of a peer to peer distributed network which will be later introduced, it becomes practically impossible to change a single block because of its well established structure and added components. The longer the chain is, the harder it becomes to tamper the block data because then any hacker will need to change all the following blocks' hashes. This property makes blockchain an immutable ledger. For this reason, governments are considering to move their traditional ledger systems like property title ledgers to decentralised distributed blockchain ledgers. For instance, blockchain has several reasons[43] to be adapted:

1. It guarantees that property titles or identity records are accurate and not tampered.
2. It reconciles transactions on a global level.
3. It is a proven technology that can potentially compete the challenges imposed by firms and centralised institutions.
4. Ledgers of contracts and capital can be decentralised and distributed in a way they may no longer require governmental support.
5. It allows depositors and stakeholders to monitor bank reserves and landing to avoid bank runs by making information more transparent and accessible.
6. It can transform bank institutions to be self regulated and self liquidating.
7. It can perform traditional regulatory functions like auditing, compliance and market operations in an automated fashion.
8. It can be a source of direct link between producers and consumers, which eliminates the need of intermediaries.
9. It is a disruption to business taxation as deregulation makes it difficult for the government to imply taxes.
10. It brings an era of human-centered capitalism and greater individual autonomy.

Distributed P2P Network

As earlier discussed, the example of the blockchain property ledger maintained by the government authority, two important questions rise: What if a person is able to change the specific block and then also changes the rest of the blocks in the ledger maintaining the cryptographical linkage? What if there's a wrong input data stored on the blockchain and restoring it might change the hash breaking the chain?. A distributed peer to peer network structure can answer these questions. It is a network composed of interconnected computers where the blockchain is copied to all the nodes. There can be millions of computers or laptops in the network. Within this framework, a property ledger may be distributed on every computer in the network. So, in this case, when a new block is added, it is communicated throughout the entire network until all the computers have this new block copied. Now, if a hacker tries to maliciously attack any entry in a specific block of the property ledger in order to illegally own a property, the cryptographical link of the chain will be invalidated. However, if the hacker has enough time and computing power to change the hashes of all successive blocks and update them with new information, he might get successful in stealing million dollars worth property. Contrary, in a distributed p2p network this couldn't be possible as the network is constantly checking and matching the blockchains of all its nodes.

In this scenario, some peers would encounter that their blockchain don't match with the attacked blockchain copy in the network. As a consequence of consensus in the majority of the nodes, the network is communicated that a hack attack has taken place. Automatically, the blocks that are being hacked are replaced by the blocks of the original blockchain. In this way, the blockchain is restored after the attack. Within this model, any hacker would have to attack at least more than 50% of the computers in the network simultaneously, and do it within a few seconds or a minute to fulfill data tampering. As it can be seen, this framework brings the concept of consensus and adds trust in the network for individuals to reliably transact between each other.

Besides the hash cryptography and the distributed p2p network, there are other levels of security in the blockchain technology that will be further discussed in the following sections.

Decentralised architecture

Blockchain is architecturally decentralised (no infrastructural central point of failure), politically decentralised (no one controls its users), but logically centralised (there is one commonly agreed set of rules) [45]. Indeed, decentralization is useful for three main reasons:

1. Fault tolerance: Decentralised systems rely on many separate components, therefore they are least probable to fail. This principle is used in real life jet engines, backup power generators in hospitals, military firms infrastructure, financial portfolio diversification and computer networks. But what if there is a common mode failure i.e. the software team gets corrupted or protocol upgraders get bribed? or client software on which all nodes of the blockchain run, get a bug?. The solution to prevent such failures is to promote a democratised protocol upgrading and developers employment as well as open auditing sessions. Moreover, mining algorithms (discussed in the next section) must reduce the risk of centralisation [45].

2. Attack resistance: These systems are very expensive to be attacked because they don't posses central points. Decentralisation becomes important when there is possibility of coercion. If one person holds 50 million dollar property worth, then only he may be threaten but if the same property is distributed among 10 individuals, it could be difficult to simultaneously attack all of them. This example represents the valuable difference between a centralised and decentralised concept.

3. Collusion resistance: Decentralised systems may alleviate most of the corporate ills. It makes harder of the leaders in corporations and governments to collude for their joint benefits that may be toxic to well-coordinated employees, customers and citizens. The institutions should not be self-interested with unitary monopolies.

Mining

As briefly mentioned in an earlier section, a block has several fields, being one of them a ”nonce” which stands for a number used only once. This field reveals what mining is all about and why thousands of mining nodes and rigs around the world are dedicating a lot of computational power to mine blocks in the blockchain. So, nonce along with the other fields of the block (block number, data, previous hash), dictates the hash of the block. All these components undergo SHA algorithm to generate hash. Nonce provides extra ability to control the hash of the block. The hash can be varied by changing the nonce but it can't be predicted with the nonce.

All the other components or fields in the block can not be changed as it may provoke data tampering which goes against the purpose of blockchain of being immutable in nature. Nonce is a 32-bit unsigned integer which has a range from 0 to 4 billion. For each bit change in the nonce value, an absolutely different unrecognisable hash will be produced, that is where the avalanche effect takes place. There is no direct or indirect proportionality of the nonce with the hash. As mentioned earlier, hash is 64 character long and exhibits a huge range of numbers. Blockchain system sets one number from this range as a target hash for the miners to achieve. Hash target can be thought of in terms of leading zeros i.e for the smaller number there will be more leading zeros and vice versa. Miners are required to find any hash below the set target to mine the block.

Miners keep iterating different nonce in order to generate a hash below the set target. Once the nonce is found at some point randomly or by brute force, which generates a hash below the target, the miner wins and that nonce is recognised as ”golden nonce”. After-then they are allowed to add a block to the blockchain and in return they get the reward, the details of which will be discussed later. Hereby, the miners are just dedicating all their computational power for churning or iterating nonce to guess the right hash.

SHA 256 cryptographical challenge because of its avalanche effect promises that the relationship between nonce and hash can not be cracked. This property of SHA keeps miners from cheating as they are unable to predict or reverse engineer the hash with the nonce. SHA256 and SHA3 are the updated versions which are stronger and more complex algorithms than the earlier versions, and are resistance to quantum attacks [6].

Mining Difficulty

It is important to understand the concepts of mining target and difficulty to get good intuition about the mining process. In mining process, the hash target is set with leading zeros e.g.

Hash Target : 0000XXXXXXXXXXXX (4 leading zeros)

which means the window for valid hashes for the miners to win the block, covers the quarter of all possible 64 character long hexadecimal hashes. In this way, more leading zeros reduces the window size of valid hashes and increases the difficulty, that means it becomes difficult for the miner to find a hash below this target hash. For example, in a decimal system:

XXXXX : 0 - 99,999 (100000 options)

0XXXX : 0 - 9,999 (10000 options)

As it can be seen, with one leading zero the options are reduced by 10. Similarly, in hexadecimal each digit has a place value of 16 therefore each leading zero will effectively reduce the pool size by 16. In order to understand the difficulty level and the probability of wining more clearly, some estimations made in below example might help. For example:

Total possible Hash 64 digit hexadecimal numbers are : $16^{64} \approx 10^{77}$
The current target in blockchain is set with 18 leading zeros, therefore
Total valid hashes (with 18 leading zeros) are : $16^{64-18} \approx 2 \times 10^{55}$

Calculating the probability A that the generated hash is valid:

$$A = \frac{2\times10^{55}}{10^{77}} = 2 \times 10^{-22}\%$$

This is extremely low probability which reflects that it is extremely difficult to meet the target and mine a block which will require a lot of computation and time. Therefore, there are big mining industries with hundreds of machines that are working day and night, solving these cryptographical puzzles to create blocks and earn rewards. Moreover, the difficulty in mining can be defined as how much harder it is now to mine a block as compared to what it was initially i.e.

$$Difficulty = \frac{current\ target}{maximum\ target}$$

where maximum target is the first ever set target in the beginning phase of the blockchain. For example, in bitcoin blockchain this difficulty is adjusted automatically by the algorithm coded inside the bitcoin protocol, after every 2016 blocks i.e. two weeks as each block is released after every approx 10 minutes [46]. Overall, difficulty is a measure of how hard it is to find a new block and it is adjusted periodically as a function of how much hashing power is deployed by the network of miners [46].

In the case of normal fiat currency, there is central authority which uses macro economic policies and based on some complex calculation process, it increases or decreases interest rates but this monetary system experiences incredibly high inflation crises. However, blockchain based monetary policy is simple and keeps all the players under-control just by adjusting the difficulty level.

Nonce

In order to understand the role of nonce in mining, extending the previous example estimations :
Nonce is 32 bit unsigned number with maximum value: $2^{32} \approx 4 \times 10^9$
This means 4×10^9 different hashes

Probability that one of this hash will be valid:

$$\text{B}= A \times 4 \times 10^{9} = 2 \times 10^{-22} \times 4 \times 10^{9} \approx 10^{-10}\%$$

However, with the whole range of nonce from zero to four billion, there is still very low probability to find a valid hash. Therefore one nonce range is not enough to mine a block. A modest miner has a computing speed of 100 millions hashes/second therefore 4 billion nonce range might take only 40 seconds. In order to reuse this nonce range, the timestamp field was introduced in the block which uses Unix [47] time and each second time changes, the hash is updated. Hence the nonce range could be reused. This strategy provides effectively infinite combinations of the timestamp and the nonce, to find the valid hash.

Mining pools

Big mining industries have more mining machines which means more computational power than the individual miners who are unable to compete in mining. In an attempt to make a fair system, mining pools were invented in which individual miners are grouped with large miner industries. In this way, hashing powers are combined by distributing work among each other. Therefore, when a mining pool wins the golden nonce, it receives the reward which is split among each party in proportion to the hashing power offered by them accordingly.

The current hash rate of mining pools in the Bitcoin network is around 70 million trillion hashes/sec [46] while in Ethereum network, it is approx. 2 thousand trillion hashes/sec [48]. According to these figures, mining pools are able to go through the whole nonce range in almost no time before even a fraction of a second is passed which means they are required to wait for a second to pass before making the next try. Therefore, the available capacity is wasted. However, to overcome this challenge, another degree of freedom is provided to the miners which is to pick the transactions and place them inside the block. In this way, they are able to change the configuration of the block which in turn changes the hash hence, the nonce range could be reused.

Memory pools

Aforementioned transactions are the unconfirmed or pending transactions stored in the ”memory pool” which is an staging area for these transactions before they are added inside the block. Every node in the blockchain network have a memory pool attached to them. All of these settings are encoded in smart algorithms that govern the mining process and provide services to mining pools such as allocating thousands of transactions for the miners. Moreover, the number of transactions per block depends on the size of block e.g. in bitcoin blockchain the block can store 1 MByte data and it normally contains 2000 transactions [48]. Furthermore, the transactions have transaction fees associated with them (explained later in following sections) which are willingly set by transacting party without any compulsion. Eventually, these transaction fees become a part of the mining reward. Therefore the smart mining algorithm in the servers of the mining pools chooses wisely transactions with high transaction fee to receive maximum reward.

Mining Machines

There are different types of mining hardware that are available for mining purposes. CPU i.e. central processing unit, a microchip installed in the computers could used for mining. However, the computational power of general CPU is limited to few MH/s (mega hashes per second) [49] which is incomparable with current hash rate which is in the scale of trillions per second. Therefore, more specialised device have been considered for mining purposes i.e. graphics processing unit(GPU) which is a graphic card found in laptops or computers and are designed mainly for solving graphical matrix operations. Thus, this specialised feature makes GPU suitable for the calculation of hash since it doesn’t have other functionalities and is only specific for one type of operation which makes it more efficient. The speed of GPU is up-to few billions H/s [50].

In 2013, first ASIC device was introduced which stands for Application Specific Integrated Circuit [50]. ASIC brought a revolution in the bitcoin industry since it was designed specifically for calculating SHA 256. This device relies exclusively on its circuit and it is architecturally designed in a way that makes very fast computation on a physical level rather than logical level. ASICs could achieve speed over 12 - 14 trillion H/s [49]. Moreover, they are very compact and smaller in size. ASIC can only be used for certain cryptocurrencies like SHA256 however, ethereum uses a different hash algorithm which is memory dependent to catch random numbers hence, the speed of calculation is limited by the access of memory speed.

Some miners rent mining hardware off premises and pay fee to the parties for participation in mining on their behalf. This type of mining also exists and known as cloud mining. One of the world's biggest bitcoin mine exist in China [7] which is based on many buildings. Each building have huge stalls of rigs installed as can be seen in Fig. 3-3, containing hundreds of mining machines, computing SHA256 and consuming a great amount of electricity. China has the most biggest mining pools due to the fact that electricity is subsidised. Moreover, electricity generation plants in China redirect their excess electricity to bitcoin miners [51].

Mining is one of the consensus protocol being implemented in the blockchain. This consensus mechanism is termed as "proof of work" which will further be a part of the next session which benchmarks different consensus protocols proposed for securing blockchain.

Byzantine Fault Tolerance

Blockchain is a decentralised ledger which means there is no central controlling authority. The valuable data stored in the ledger makes it vulnerable to attacks. Bad actors in the system could take huge economics benefits by creating faults and frauds.One of the notable fault identified is Byzantine Fault in which some nodes could send conflicting information to the different parts of the distributed network. This fault is named Byzantine because it is exemplified in terms of generals in byzantine army camped around an enemy city [52] where generals have to communicate via messages to agree upon a common battle plan. However, there are traitors among them who may try to confuse others and this situation is termed as Byzantine Generals Problem

Figure 3-3: Inner view of China's Biggest Mining Industry [4]

[52]. Therefore, an algorithm is required so that loyal generals doesn't get mislead by the traitors and can reach to an agreement to make a right decision.

In this pursuit, an algorithm known as byzantine fault tolerance(BFT) has been presented which takes the majority of the conveyed information and reaches to consensus in order to avoid misleading messages. However, this algorithm works only if there are not more than 33% traitors in the system which means in an army of ten generals, there should not be more than three traitors otherwise consensus can not be reached and armies will be unable to coordinate an attack. Thus, in a blockchain decentralised system, without BFT, dishonest nodes are able to transmit or post false transactions in the block and there is no central authority to fix these faults. However, there are more secured algorithms or consensus protocols required for protection against such byzantine faults which must be tolerant beyond 33% attacks, as much as possible. Byzantine fault tolerance(BFT) is a very old concept and is also used today in airplane engine systems, rockets in space station and other similar systems where components could be termed as generals. Therefore, malfunctioning of any component in such systems doesn't cause the failure of the whole system.

Consensus Protocols

Blockchain distributed network requires some consensus mechanism to update its ledger or to add a new block to the chain, because of some uprising challenges to its security and data privacy. As mentioned in BFT example, it was a challenge for the generals to understand and decide to attack or retreat because of conflicting messages. In the case of blockchain, consensus protocol is required to mainly solve two challenges, the first one is to prevent attackers to add malicious block in the blockchain. The second challenge is that, if there is lag between two nodes far away from each other, successfully mine a block simultaneously and the network doesn't come to consensus then it results in conflicting chains.

In order to address these challenges, different types of consensus protocols have been designed and proposed for the blockchain technology. One of the famous and widely used consensus algorithm is Proof of Work(PoW) which was first proposed by Satoshi Nakamoto, the founder of blockchain in the paper [19]. Moreover, currently big blockchain platforms like bitcoin and ethereum are implementing PoW as a consensus protocol.

Proof of Work

This protocol has already been discussed in details in the mining section which has laid down the very basic features and functionalities of this algorithm. Miners have to spend a lot of money on electricity for mining as it takes a lot of computational power to solve challenging cryptographic puzzle. They have to proof their work in order to receive valuable reward i.e. financial incentive.

Proof of Work (PoW) is designed in a way that restricts the winning miner to add a malicious block. In the case of fraud, he will loose his reward and won't be able to pay huge electricity bills. When a new block is generated and propagated across the blockchain network, each node conducts a series of rigorous checks or verification which is not a computational heavy process. Thus, it is hard to solve a cryptographic puzzle but easy to verify. In this way, PoW addresses the first challenge to the blockchain.

In the case of conflicting blockchains i.e. byzantine fault which is the second important challenge, the consensus protocol works in the same manner like BFT but with a different approach. The competing chains wait for the next block to check which chain adds the block first and gets longer. The longer chain is then considered valid and copied to all nodes in the distributed network. The key to succeed in the consensus mechanism is to own the highest hashing power to generate the longest chain. The consensus protocol means that consensus of 51% of the hashing power of the network is required to compete and be considered as a valid chain. This protocol is more powerful than BFT which requires 70% honest players to reach consensus.

Apart from the advantages of PoW, mining process consumes a great scale of electricity therefore majority of mining is centralized in those areas of the world where electricity is cheap. But blockchain demands more energy-efficient and less centralised consensus algorithms. So there have been different alternative approaches explored. Some of the significant ones are discussed this section.

Proof of Stake(PoS)

One of the famous alternative to PoW is PoS in which a miner instead of investing in the mining machines, holds the stake i.e. native digital currency in the blockchain network [53]. Cryptographic hash difficulty doesn't exist in PoS. Miners get the chance of creating next block based on their shares in the system e.g. a miner holding 300 coins, has three times more chances of mining the next block than the miner who holds 100 coins stake. PoS secures the membership of the players and are grants each of them their turn to play e.g. if a miner didn't get a chance to mine a block because of less stakes then his membership time will be counted as another factor. When a new block is created, it undergoes signing process and is verified by each node. Based on majority vote, the block is declared valid and added to the chain. However, if a miner tries to double-cross, he will loose all his holdings. Peercoin [54] is the first blockchain to implement this consensus protocol. Moreover, ethereum is also shifting from PoW to PoS [55].

All the other proposed consensus protocols revolves around the same goal i.e. to improve the efficiency of BFT and PoW. For example, Proof of Activity is a consensus algorithm which combines the features of PoW and PoS to increase the efficiency. Proof of Elasped Time consensus mechanism uses relaible devices which consumes less electricity as compared to that in PoW. Proof of Authority consensus is a combined improved version of PoS and PoW that allows only few trusted nodes known as validators, to validate the transactions and create blocks. Thus, this appoarch increases block generation rate while reducing energy consumption and computational complexity [56]. Proof of Capacity/Storage suggests nodes to invest their hard-drive space instead of investing money, to become a part of the network. There are even more proposed consensus protocols however, there is still a demand of more work to practically design and implement these protocols.

The architecture and critical characteristics of the blockchain have been introduced in a comprehensive way. It can be concluded from the discussion so far, the phenomenal properties of blockchain technology make it a powerful tool for the transformation of existing industries infrastructures.

3.2 Types of Blockchain

According to the nature of blockchain applications, it is categorised into following:

- Public Blockchain: As the name suggests, this type of blockchain is open and accessible to public i.e. all the nodes in the network. Anyone can participate in the consensus process. Public blockchains are fully decentralised which doesn't allow changing and revoking the transactions after they are stored in the public blockchain. This blockchain implements most commonly used consensus algorithms e.g. PoW and PoS.

- Private Blockchain: This type of blockchain allows only its owner i.e. higher authorized node to access and change the data which means write permissions are centralised to one organization [57]. On the other hand, rest of the nodes have limited access over the private blockchain. There are only some designated nodes who are allowed to validate the transactions. Moreover, the transaction costs are less in private blockchain as comparable to public blockchain. This type is applicable to the closed group areas such as intranet. Most commonly implemented consensus mechanisms in private blockchains are Practical BFT and Raft [58].

- Permissioned Blockchain: This type of blockchain combines the characteristics of public and private blockchains, in terms of centralization and accessibility. It is designed for the semi closed network composed of many parties or enterprises where consensus process is controlled by nodes which are pre-specified by participants e.g in a consortium of 15 financial institutions where each one is operating as a node, there are 10 selected nodes among them who must be in consensus to approve a block. Validity of transactions is dependent on the majority vote of consensus nodes. However, the parties do not fully trust each other in this type of blockchain network. PBFT is usually implemented as a consensus mechanism in the environment where parties may have conflicts [58].

As shown in Fig.3-4 public and private blockchains can be permissioned or permissionless. Permissionless blockchain allows anyone to participate in the network e.g bitcoin and ethereum are public permissionless blockchains where anyone can join the network and participate. In addition, there is hybrid combination of private and public blockchains which is known as federated blockchain which combines the properties of both types of blockchains to enable a partial decentralised design where authorised nodes could allow permissions to the other users [6].

In order to avoid any confusions between the terms, it is important to know that the technology, protocol and tokens are the three different layers of revolutionary decentralised system. As illustrated in Fig.3-5 the first layer i.e. blockchain technology which has already been discussed so far. The second layer is the protocol

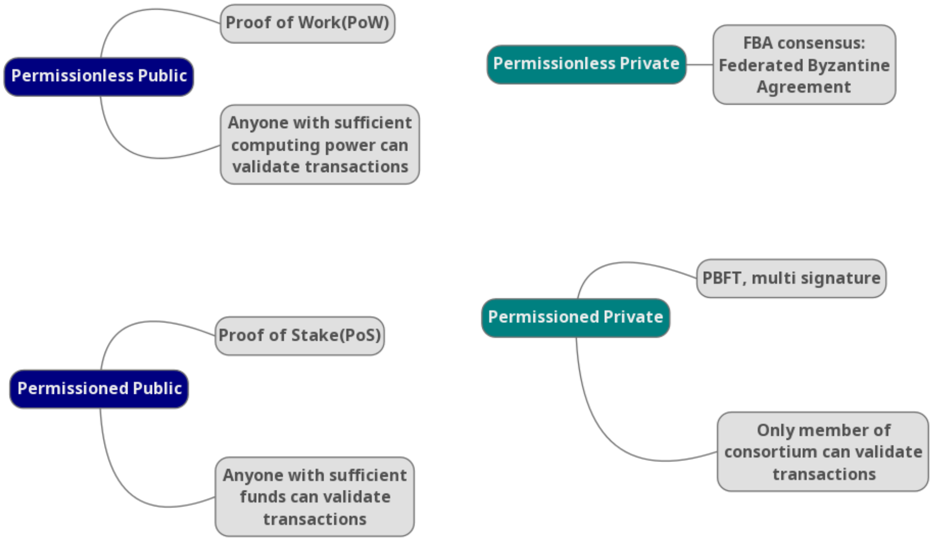

Permissionless Public
Proof of Work(PoW)
Anyone with sufficient computing power can validate transactions
Permissionless Private
FBA consensus: Federated Byzantine Agreement
Permissioned Public
Proof of Stake(PoS)
Anyone with sufficient funds can validate transactions
Permissioned Private
PBFT, multi signature
Only member of consortium can validate transactions

Figure 3-4: Types of Blockchain [5]

which is the set of rules defined for communication between the participant of the network, just like IP protocol allows us to communication over internet. For example, ethereum and bitcoin are among several protocols which are designed for blockchain technology. Moreover, protocol dictates consensus as it allows the participants of the network to communicate in order to achieve consensus. Furthermore, it also dictates that how the public keys and signatures should be used for authentication. Besides, all protocols have their own coins which are innate assets, to facilitate the interaction of players with the blockchain platform for mining or trading purposes, and are also used as a block reward. Moreover, some protocols create tokens which forms the third layer. Tokens rely on smart contracts e.g. ethereum is the most popular protocol for creating tokens and smart contracts. However, all of the protocols does not facilitate smart contracts. Tokens introduces disruption in other industries.

3.3 Applications

Based on the capabilities and disruptive potentials of blockchain technologies, a wide range of industrial applications have been explored and under further research and

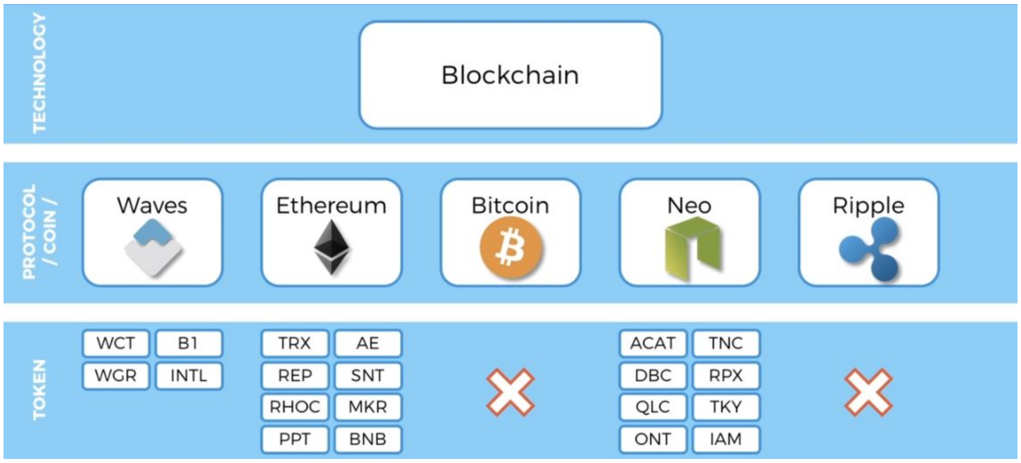


Figure 3-5: Layers of Blockchain [6]

development. These applications span diverse fields like financial sectors, healthcare, supply chain, governance, digital data management, energy sector and many others [11].

3.3.1 Financial markets

The biggest success of the bitcoin blockchain grabbed the attention of the world and reflected that the promising features and services of blockchain could be applied to the financial markets. These blockchain enabled applications could facilitate business services, financial asset settlements, digital transactions, financial contracts, auditing services and more. Blockchain based frameworks for financial market operations are being under continuous research and development. The world's biggest banks including Barclays, have shown interests to deploy these frameworks which will lead to huge cost savings [6].

3.3.2 Healthcare

Blockchain technology could potentially revolutionise the healthcare industry with variety of application services like electrical healthcare records maintenance and management, automated health claims services, online access and data controllability for patients, healthcare data exchanges, user oriented medical research etc. Current healthcare systems have inconsistent, unsecured and centralised medical data storage which gives an advantage to the hackers to breach the patient data. In contrast, the advantages of electronic healthcare records are that they are stored in a distributed way which provide resiliency against data breaching because the data is preserved in the secured ledgers. Doc.ia and encrypgen are few of the blockchain based healthcare startups who have developed several healthcare data solutions [59].

3.3.3 Supply chain

The combined capabilities of IoT and blockchain are promising to resolve many issues related to current supply chain management with increased traceability and accountability in the supply chain networks. These combined technologies brings breakthroughs in different areas of supply chain such as logistics tracking mechanisms, provenance of goods, traceability assurance, information management, enable direct dealing between producers/designers and customers without involvement of intermediaries. IoT and blockchain merger has given birth to many companies such as Provenance, Everledger, Smartlog and others, which are deploying these technologies to provide innovative digital supply chain management solutions [59].

3.3.4 Governance

Blockchain enabled applications are equally compelling for governments, bringing transformation in the government roles, services and its structure. These applications offer management of the official records of the citizens or enterprises in a decentralised and secured manner which could avoid corruption and provide secured governance services. Property title registrations, marriage registrations and passport services are the few of the government services that could be transformed with blockchain applications. The World citizen project is an example of a decentralised passport service [6]. In Hondrus, property titles have been digitized by using blockchainledger technology [59] . However, blockchain governance implementation is a big challenge for the current government authorities who posses control and management, because blockchain brings a decentralised system with no third party intervention [11].

3.3.5 Energy sector

Blockchain also finds its application to serve energy sector. There are several use cases of blockchain in the energy sector which includes decentralised P2P energy trading, DR demand response services, network management and control, coordination of virtual power plants with grid, management of energy storage systems, community energy projects, control of decentralised energy and coordination of RES power plant portfolio [13]. Several research initiatives, companies and collaborations have been focused on the development of these applications to improve overall efficiency and economy of the existing energy systems. Since, this thesis is based on P2P energy trading therefore upcoming sections will form the basis for the development of P2P energy trading model. The blockchain based applications are extended to far more domains as illustrated in Fig. 3-6 other than those discussed above. Moreover, there is a fast paced research work in progress, to explore more capabilities of this technology. Furthermore, crowd funding platforms are welcoming innovator and developers from around the world to shape their innovative ideas into real applications using blockchain frameworks.

3.4 Blockchain Paradigms

Till now the blockchain structure and taxonomy have been discussed in order to understand the operation of blockchain technology. Furthermore, the two important blockchain paradigms will be explored in this thesis i.e. Bitcoin which is the first and largest blockchain application, and Ethereum blockchain platform which supports the development of majority of the energy applications.

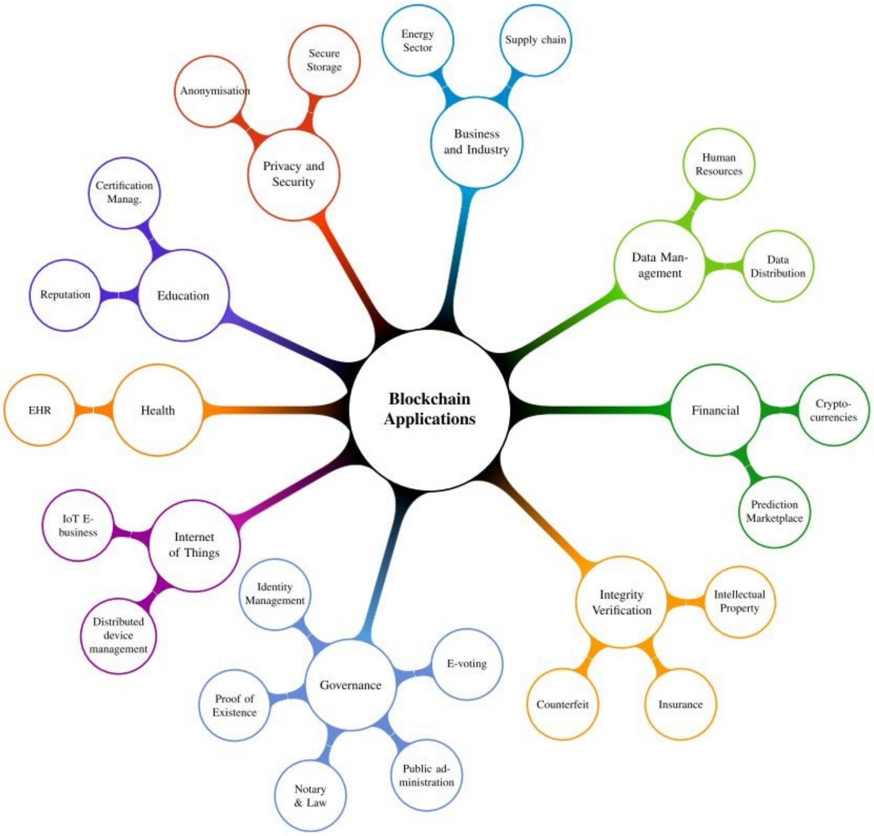


Figure 3-6: Applications of Blockchain [7]

3.4.1 Bitcoins

Bitcoin was the first practical implementation of blockchain theory presented by Satoshi Nakamoto in 2008 [19]. The idea was to make a financial system independent of any intermediaries such as centralised control of banking sector is not required anymore, thus adding transparency in the system. The ecosystem of bitcoin network is composed of nodes, miners, mining pools and large mines.

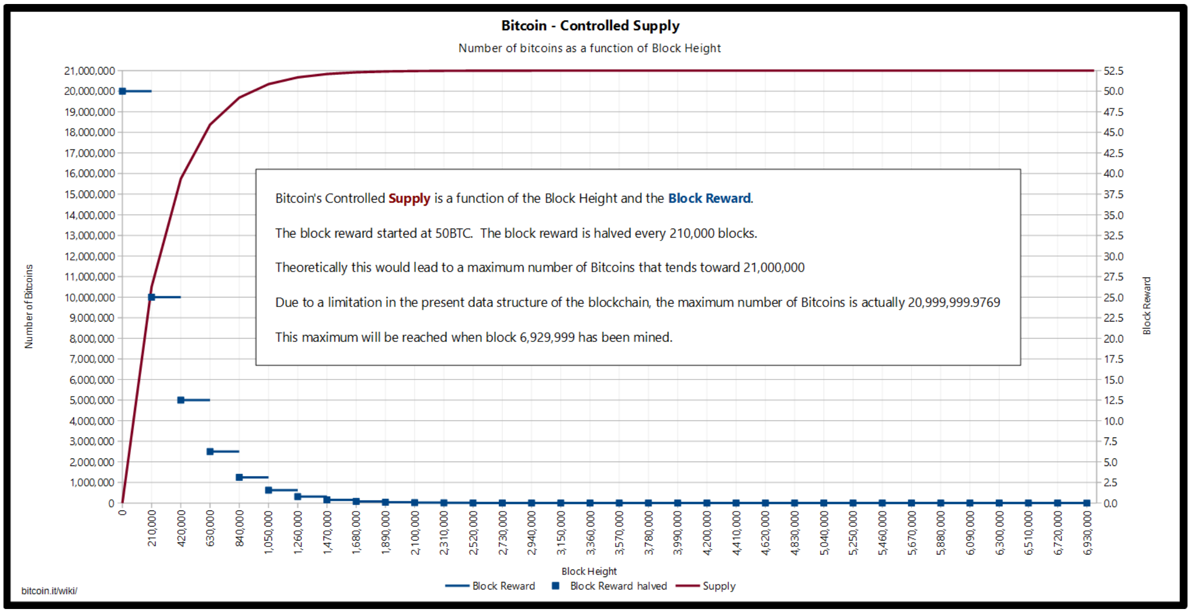
Bitcoin holds its own coin i.e. cryptocurrency and monetary policy which is entirely software based i.e. pre-programmed algorithms, structured over two main parts:

Halving scheme

Bitcoins are released as reward when a new block is generated. These bitcoins per block are halved after every 4 years. Transactions fees are meant to replace the block rewards.

Total mining reward = Bitcoins per block + Transactions Fee

As the time will pass, there will be more players joining the bitcoin platform and thus more transactions will be executed that means more transaction fees. Moreover, participants will pay high fee for their transactions to be picked and added into block. Therefore, bitcoins per block are reduced to keep the reward stable as major part of the reward will come from transactions fees. By 2140, final bitcoin will be released and there will be 21 million bitcoins in circulation as can be seen in Fig. 3-7.



Bitcoin's Controlled **Supply** is a function of the Block Height and the **Block Reward**.

The block reward started at 50BTC. The block reward is halved every 210,000 blocks.

Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000

Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769

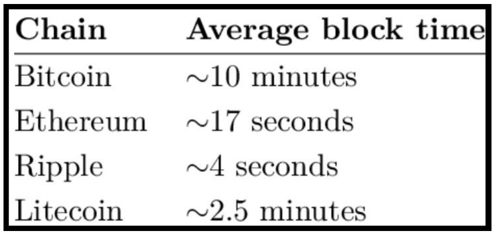
This maximum will be reached when block 6,929,999 has been mined.

Figure 3-7: The Halving Scheme of Bitcoin [8]

Block Frequency

Design structure of the system and the number of participants, governs time required to generate the next block in the chain. This varies for different protocols as seen in Fig.3-8 e.g. in bitcoin, average time difference in blocks creation is ten minutes which is higher than other blockchains because of the large number of participants and transactions.

Bitcoin is a fundamental restructuring of the monetary systems as it is a market



Chain	Average block time
Bitcoin	∼10 minutes
Ethereum	∼17 seconds
Ripple	∼4 seconds
Litecoin	∼2.5 minutes

Figure 3-8: Block Frequency [9]

based solution to the debt-based money supply. It is a deflationary kind of cryptocurrency or inelastic which means a specific amount of bitcoins will be created. This cryptocurrency is decentralised, transparent, open source, based on computation and consensus mechanisms that brings disruption to the centralised, opaque and debt-based current monetary regime [60]. Bitcoin is an existential threat to incumbents such as regularities of the financial sector.

3.4.2 Ethereum and Smart Contracts

Vitalik buterin in 2014 after the introduction of bitcoin blockchain, came up with some innovative idea to enhance the capabilities of the blockchain technology. He proposed that the blockchain is not just restricted to store transactions however, it can also facilitate the execution of programs over the ledger. The core idea was to build a super computer in a distributed manner where all the nodes in the network are executing programs and applications. The programs are stored in the blocks just like transactions and any changes happening in the programs are also recorded in an immutable manner. He introduced Ethereum platform for others to create programs and build projects over it. This platform provides infrastructure for writing smart contracts and build decentralised applications where anyone can implement their own functions, rules or clauses, terms and conditions to carry out any operation [61]. Ethereum has its own coin named "ether" which allows users to invest, transact and create smart contracts and applications over the blockchain network.

Smart Contracts are the automated executable scripts or codified tasks which are subjected to the certain conditions. In other terms, smart contracts are the set of rules and clauses that parties agree upon, which governs the relationship between them. The programming language used in bitcoin is called bitcoin script which allows coding on blockchain. In ethereum, solidity is used to write smart contracts.

Solidity

It is a Javascript like general purpose language, designed by several Ethereum core contributors. It is a statically typed contract language which contains state variables, functions and common data types. With solidity, developers are able to write business functions in a smart contract to create decentralised applications(DApps) [62].

The difference between bitcoin script and solidity is turning-completeness which means any logic can be codified into that programming language. Bitcoin script doesn't support every logic e.g. loops can not be implemented and that is done intentionally because the blockchain runs on every node in the network. In this case, if there would be any infinite loop encountered then it would cause the delay in the system and destroy the whole blockchain. However, ethereum posses all the required elements to facilitate any logic therefore, it exhibits potential for coding and running programs over the blockchain.

Ethereum Virtual Machine

Smart contracts are executed by turning complete Ethereum Virtual Machine(EVM) which is an ethereum's runtime environment that runs on every node in the network. Nodes which are actually computer systems, are prone to many attacks and risks. Most evident risks and security threats are as follows:

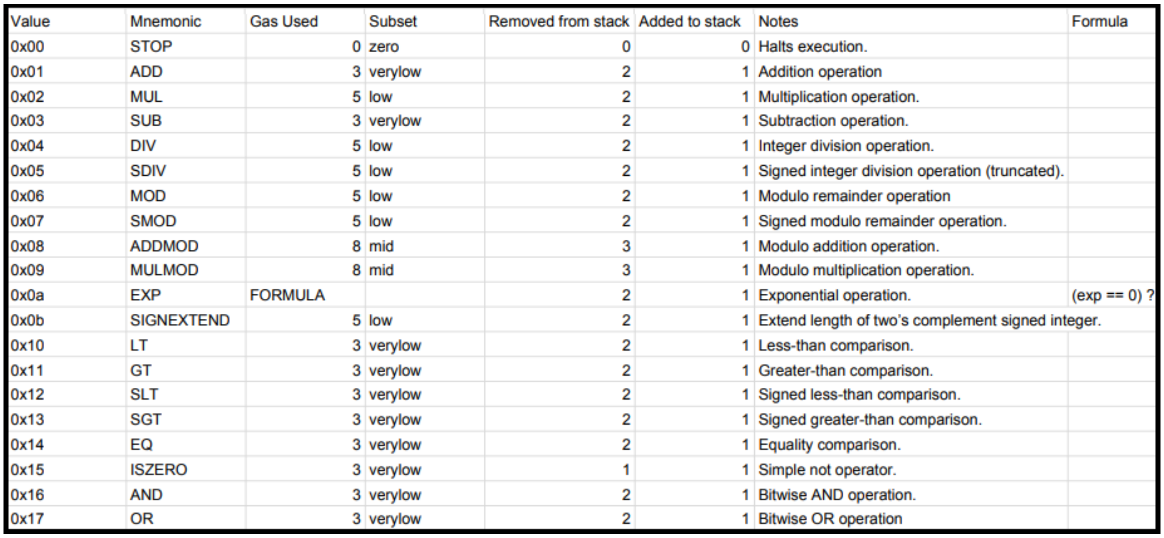
1. Viruses can be inserted into smart contract by anyone. In a distributed environment as smart contracts run on every single node, virus is convenient to be copied to all nodes. In this way, smart contracts may gain access to the private files of the machine.

2. Infinite loops or heavy computations in smart contracts may cause delays and slow down the whole network as highlighted earlier.

EVM presents solution to the first security threat. Since, it runs into the computer and encapsulates the running smart contracts. Therefore, it ensures anything running on machines stays inside the boundary and secluded from other parts of the machines. In this way, privacy is saved and smart contracts may never have access to other private files of the computer system.

Gas

Ethereum introduced the concept of gas which is an ingenious solution to the second risk mentioned earlier. For any computation that runs on the blockchain, the developer of the smart contract is required to pay gas for it. Notion of gas is like a fuel running the whole system and it is similar in notion to the consumption of gas by the moving car. For each logic operation, there is a specified gas price which can be seen in Fig.3-9.



Value	Mnemonic	Gas Used	Subset	Removed from stack	Added to stack	Notes	Formula
0x00	STOP	0	zero	0	0	Halts execution.	
0x01	ADD	3	verylow	2	1	Addition operation	
0x02	MUL	5	low	2	1	Multiplication operation.	
0x03	SUB	3	verylow	2	1	Subtraction operation.	
0x04	DIV	5	low	2	1	Integer division operation.	
0x05	SDIV	5	low	2	1	Signed integer division operation (truncated).	
0x06	MOD	5	low	2	1	Modulo remainder operation	
0x07	SMOD	5	low	2	1	Signed modulo remainder operation.	
0x08	ADDMOD	8	mid	3	1	Modulo addition operation.	
0x09	MULMOD	8	mid	3	1	Modulo multiplication operation.	
0x0a	EXP	FORMULA		2	1	Exponential operation.	(exp == 0) ?
0x0b	SIGNEXTEND	5	low	2	1	Extend length of two's complement signed integer.	
0x10	LT	3	verylow	2	1	Less-than comparison.	
0x11	GT	3	verylow	2	1	Greater-than comparison.	
0x12	SLT	3	verylow	2	1	Signed less-than comparison.	
0x13	SGT	3	verylow	2	1	Signed greater-than comparison.	
0x14	EQ	3	verylow	2	1	Equality comparison.	
0x15	ISZERO	3	verylow	1	1	Simple not operator.	
0x16	AND	3	verylow	2	1	Bitwise AND operation.	
0x17	OR	3	verylow	2	1	Bitwise OR operation	

Figure 3-9: Gas costs for Operations [10]

Solidity code is first converted to low level computer language and then prices are applied corresponding to each logic operation. Therefore, if the code is computational heavy then developer will get short of gas units and program will not be executed. In this way, heavy computations will not impact the operations of the blockchain. This is an smart way of keeping the blockchain safe as well as motivating the developers to write efficient codes in the smart contracts. Moreover, Ethereum uses gas instead of ether because of the fact that ether fluctuates and is unpredictable. The conversion rate between the gas and ether is decided by the consensus of the ethereum community in some way.

Decentralized Apps (Dapps)

Dapps function in a similar fashion like other web applications which are designed and written for serving users for different purposes. For example, there are applications available for online banking, car riding, socialising, gaming and so on. Since, all of the traditional applications are running on the central servers and have centralised databases. Therefore, in the cases when servers go down or if they are hacked, the entire system is hugely affected and results in massive loss. Whereas, Dapps have great advantages over traditional applications. As named, these applications are decentralised which means they run on a P2P network of computers, instead of a one computer.

Dapps consist of a front end and a back end. Front end provides user interface which is similar in appearance to that of regular apps in most cases because it uses typically HTML or JavaScript web applications to interact with blockchain [55]. Whereas, on the back end there is a smart contract which provides application programming interface (API) for applications to interact with blockchain. The interoperability between front and back end is provided with web3.js ethereum JavaScript API. Moreover, dapps are open source which means anyone can view the front end and back end application codes unless the developer keeps his code private for confidentiality purposes. Steemit [63] is a dapp which functions just like a twitter but it is totally decentralised. Storj [64] is another an excellent innovative dapp under development, which intends to provide decentralised cloud storage. Multiple types of promising dapps are being created and under development, serving diverse fields such as financial, governance,health,education community and energy [65].

Decentralized Autonomous Organizations (DAOs)

DAO concept first came into being based on the idea of replacing humans in organisation with smart contracts to automate by codifying the operations, procedures, rules and regulations, protocols definations that may no longer need entities such as board of directors, managers and employees. For example, assuming a DAO Ride Service, where cars are automated self driving which picks up the passenger and drops him off to the destination as per the operations defined in the smart contract embedded in the organisation. Moreover, in this service, smart contracts governs how it interacts with the smart contracts of petrol station for fuel purchase exchange. In this fashion, there is no requirement of human intervention for the running the operations of the organisation however, it does require certain set of members or shareholders with 67% majority to decide the allocation of investor-directed venture capital funds [66]. DAO is capable of expanding on its own because of the logic coded inside its smart contract e.g. when the revenues hit the threshold, organisation keeps on surviving even if the starters are no longer interested. It can be described as a virtual entity that exist on internet autonomously but relies heavily on certain set of members or shareholders to execute certain tasks that can not be handled automatically.

In 2016, Vitalik along with others jointly established a DAO on etehreum, the concept behind was to create investor-based venture capital funds to help organisations for the development of decentralised applications. In may 2016, ethereum team crowdfunded for the DAO through a token sale. It was the most successful crowdfunding campaign in history as it raised 150 million dollars worth. However, there was a flaw identified later in the code of DAO's smart contract when an attacker hacked 50 million dollars in june 2016 [67] and transacted money from DAO account to his account openly and legally. But because of the immutable nature of the smart contract, it was not possible to amend or rectify the flaw at that moment. A big dilemma appeared that ”code is law” according to one part of the member's community who were not in favor of changing deployed DAO smart contract whereas, the other part of community was of opinion that lost money belongs to the people and decided to make a hard fork (discussed in next section). This resulted into a new Ethereum(ETH) while old ethereum classic ETC is in its place running with the hack included.

Hard and Soft Forks

Etheruem blockchain was hard forked in July 2016 [68] and split into ETH and ETC as a result of flaw identified in the smart contract code which became responsible for the big financial loss in an attempt of attack. It is termed as hard fork because of it's physical nature, community was split into two after the blockchain fork. Hard fork can be considered like a software upgrade, for those who upgrade to new version may enjoy the new added features while others may keep using current version as they are not forced to adopt it. Hard fork implements loosen rules and is flexible, to respect opinion and right of everyone in the community. Another hard fork happened with bitcoin in July 2017 [69] when it accepted segregated witness or Segwit, a technical advancement in which signatures were stripped out from the block and sent separately through the network via special message services. The reason was to make more space of transactions in block by removing heavy part of the message called Scriptsig i.e. signs and public keys occupying 60% of transactions space. Some member showed resistance to accept this change. However, with the majority consensus, the team made soft fork in the chain on 20 July 2017 and implemented segregated witness. However, the opposing minority decided to upgrade to 8 Mbytes block size which resulted in the hard fork which happened on 1st august 2017 [69], the bitcoin split to bitcoin and bitcoin cash, they joined bitcoin cash.

Soft fork brings tighten rules which are required to be followed by everyone in the network. As earlier mentioned, bitcoin made segwit soft fork [69] which was accepted by majority of members while others had to face challenges like orphaned block situations. When two miners produces the blocks simultaneously, only one block is validated and added to the chain, based on the higher number of transactions. Whereas, the other block is detached from the chain and is known as orphaned block, This scenario signifies the miners with segwit who will win every time because of higher capacity of blocks for transactions. As a result, this situation forces minorities to accept new rules and in the same way, segwit soft fork was accepted in bitcoin. Thus, soft fork ensures backward compatibility.

Initial Coin Offerings(ICO)

ICO takes place on two different layers of the blockchain, the protocol layer and the token layer. Most commonly, ICO is carried out in the token layer in which token sale is conducted. When a party or enterprise have any innovative business idea or startup plan to build any application using blockchain platform, they execute ICO to collect funds for the development and growth of their projects.

To understand ICO concept well, it is significant to identify IPO and its comparison with ICO. IPO is an initial public offering that have been used by the companies to raise money from stock market where the shares are available to general public. Founders of the company conducts IPO for startups or to scale their businesses where public gives cash to the company and become shareholder of their business. However, this entitlement provides shareholders the control and profit share in the company. Whereas in ICO, the founders or innovators, to increase their capital and establish their company, show cases their business idea, products and services in an enclosed environment and introduces their own tokens which can be bought in exchange of fiat currency. In initial stage, the price of tokens are kept low but later when the business starts growing these token's value goes high. Founders conduct limited tokens sale for the public so that those investors who have interest and believes in the potential of the idea and the business growth in future, buys these tokens. In this way, founders may increase their capital to deploy and scale their businesses. Token value increases with business growth hence, investors may sell their tokens to the public who wants to avail the services and products of the company. In this way investors may earn profits over the tokens unlike IPO in which they get control over the business and its revenues. Hence, using ICO, the founders may remain in full control of their assets and revenues and receive full autonomy over their businesses. In the same way, Dapps and DAOs conduct their token sales in their initial phases to grow their businesses.

Indeed, ICO is an advanced form of entrepreneurship.

Blockchain technology has been evolved a lot since its origin and still in the phase of further developments. Three generations of blockchain are identified depending on the targeted audience. As depicted in Fig.3-10 Blockchain 1.0 is the first generation, the embryo stage when bitcoin blockchain was introduced. This generation includes applications which supports digital cryptocurrency transactions. Blockchain 2.0 is the second generation in which smart contract technology was introduced by Ethereum, which supports development of decentralised blockchain applications which are extended beyond just cryptocurrency transactions. Blockchain 3.0 is the third generation which includes set of blockchain-based applications in other diverse fields such as governance, law firms, healthcare, society and others.

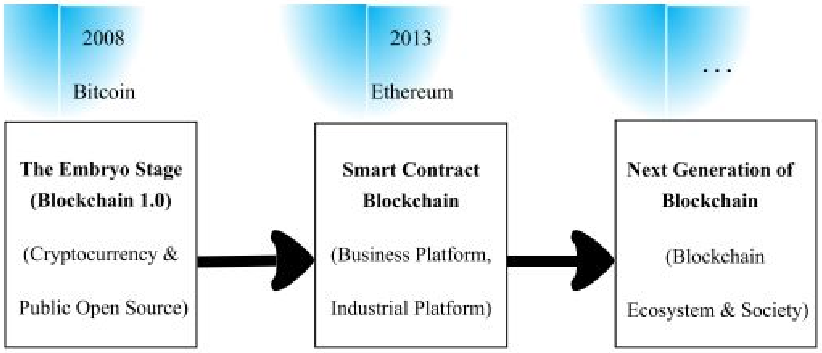

2008
Bitcoin
2013
Ethereum
. . .
The Embryo Stage (Blockchain 1.0)
(Cryptocurrency & Public Open Source)
Smart Contract Blockchain
(Business Platform, Industrial Platform)
Next Generation of Blockchain
(Blockchain Ecosystem & Society)

Figure 3-10: Blockchain Generations [11]

3.5 Challenges, Risks and Security Concerns

Evidently, blockchain technology displays promising benefits which could bring industrial revolution with powerful characteristics and phenomenal services. However, there are some challenges, risks and security concerns related to this technology which limit its adaptability in the mainstream. Some reviewed concerns are summarised as follows:

Quantum attacks: The fast paced developments in the quantum computing imposes future concerns to the the blockchain which implements encryption algorithms.

Once a big quantum computer is built, it can crack the ECDSA algorithm, applied in blockchain for private key encryption thus raising insecurities in all blockchains [6]. Therefore, blockchain requires advancements and developments to make these algorithms strong to resist quantum attacks. In this run, SHA 256 algorithm shows resilience towards these attacks. Moreover, there are on going developments on post quantum cryptography which may be shatter-proof to quantum attacks [70]

Smart contracts: Smart Contracts are vulnerable to bugs and fraudulent activities because of the transparency of the blockchain technology and its distributed P2P network structure. Since, ledgers are copied to all nodes, they are susceptible to viruses embedded inside the running smart contracts. The irreversible nature of the blockchain, makes it challenging to revert back the smart contracts once deployed. Famous DAO attack in 2016 is an outstanding example of this challenge (as discussed earlier in detail) which resulted in Ethereum hard fork. Therefore, in this context, improvements are required in the blockchain framework such as strict checks and verification to authenticate the smart contracts.

51% Attack and Selfish Mining: Blockchain is an immutable, temper-proof and distributed ledger system which implements consensus mechanism to prevent tamper attacks. However, if an attacker holds control over 50% mining nodes then it is possible to hijack the entire blockchain and add malicious blocks. Moreover, the history of all the transactions record can be revised or forged. In contrast, there is another type of attack that may happen even when miner posses mining power less than 50% of network. This strategy is known as selfish mining, in which the miner keeps adding mined blocks in the blockchain offline to achieve the greatest length of the blockchain and then suddenly gets online, where consensus mechanism as of its rule that the longest chain wins, considers his chain valid and replaces all the blockchain copies across the network. In this way, the attacker loots the mining reward and also attracts other miners to join his network with common interests. Hence, these types of threats need to be considered and handled to maintain resiliency and security of the blockchain.

Privacy Leakage: There are still privacy and confidentiality issues in the public blockchains which provide transparency and traceability of the transactions and smart contracts operations [6], to everyone across the network. Attackers may take advantage of these properties of blockchain and could track users information to hack accounts and make frauds. Although blockchain uses pseudonyms and encryption based mechanisms to provide data privacy. However, blockchain doesn't provide satisfying solutions to prevent tracking and the disclosure of the sensitive information [71].

Chapter 4

Transactive energy using blockchain

With the advent of the smart grids concept, the requirement of the two way grid management has emerged for enabling energy transactions among all participants [72]. A significant growth of prosumers has been observed who demand for participation in the electricity market using their ability to inject the excess produced energy into the grid and in return receive some profit or reward. This emerging trend gave rise to the transactive energy paradigm. A decentralised vision for the power grid operations, in which peer to peer local energy trading within the distributed network can potentially reduce the strain on the network operators, leading towards the development of Transactive Energy (TE) platform [13]. In this regard GridWise architecture Council proposed a definition for transactive energy, i.e. "a system of economic and control mechanisms that allows the dynamic balance of supply and demand across the entire electrical infrastructure using value as a key operational parameter" [73]. This definition refers the value, as the reward or incentive for the participants.

The transactive energy platform provides a unique distributed local energy market model(LEM) where participants can be aggregated for flexibility purposes [74] thus improving system reliability and efficiency of the power system. LEMs have the potential to empower prosumers with additional revenue streams and consumers with reduced energy costs. Different transactive energy schemes and architectures based on transactive controllers along with the usage of intelligent devices, such as smart meters in smart grids, have been proposed to support the bidding process, trading operations and activities of the participants in LEM [75, 76]. Secure and privacy-preserving protocols have been designed [75] for these transactive energy systems, as all the transactions are processed in a decentralised way. Thus, TES can turn traditional power grids into modernised grid which avenues potential services and facilitates the collaboration of the participants in the network. Over the last few years, a series of transactive energy based pilot projects have been presented as well [77, 78, 79]. Soon, the research studies on transactive energy modeling will reveal more potentials of this energy ecosystem and pave the way for practical implementations that will evolve traditional distributed energy resource management and facilitate decentralised balancing models [80] to increase distribution system efficiency. Next sections explain how the transactive energy platforms based on emerging distributed ledger technologies may seriously disrupt the existing the energy market structures.

4.1 Challenges to Centralised Architecture

Traditional power systems are based on centralised architecture where they have centralised servers for the management of operations like monitoring of energy consumption and production, energy pricing, billing, authorization and maintenance of the secure record of all energy transactions. However, the increased penetration of prosumers into electricity market will create high volumes of data at a high frequency. In order to handle this energy data, the scalability of centralised architecture is required which is not easy to achieve as it leads to high integration costs which makes the architecture not economically feasible [18].

Moreover centralised management also induces intermediary costs and demands participants to trust third party to handle operations on their data. Furthermore, the centralised servers are also subjected to a single point failure situation which makes them sensitive to malicious attacks [13]. Therefore, the need of time is to introduce the transactive management infrastructure which must posses strong immune system to such failures. In addition, some advanced features [18] are required to collaborate with the divergence of DER assets such as:

1. Privacy preservation: Since all the participants entrust and share their profiles with the third party in order to make an energy exchange therefore, data confidentiality is lost.
2. Data Security: Financial transactions are being exchanged hence, security is required.
3. Large scalability: Increasing number of prosumers in the market demand scalability.
4. Small energy footprint: Infrastructure is not energy efficient.
5. Resilience: Single point failures and attacks are the main threats to the centralised systems.
6. Speed of financial transactions settlement : Centralised servers are loaded with large data which reduces their speed of operations.
7. Traceability: traceability of complete trail of transactions is not available.

4.2 Blockchain based P2P Transactive Energy Systems

As reviewed in the previous chapter, the powerful characteristics of blockchain ledger technology makes it best suitable to meet all the challenges pertaining to traditional power systems. Blockchain presents peer to peer decentralised architecture for energy exchanges which exhibits a wide range of advantages over traditional centralised architecture of the power systems. Blockchain offers innovative P2P energy trading platforms that allows beneficial energy exchanges among participants in a P2P fashion i.e. prosumers can sell their excess energy and consumers can buy energy at a reduced cost. This paradigm shift towards decentralised P2P local energy trading will immensely reduce the transmission losses and also defer expensive upgrades in the network [13]. Contrary to the centralised servers in centralised architectures, the blockchain ledger is distributed and replicated across the network and eliminates the third party involvement [13]. Thus, this technology ensures integrity and security of the system. Blockchain uses automated smart contracts technology to execute, process and record all transactions to an immutable, transparent and tamper-proof secured ledger. Hence, it improves cybersecurity and optimises the energy processes which could significantly reduce the transaction costs. Along with IoT applications, this decentralised architecture can offer more flexible and efficient energy markets which in turn add resiliency to the power system network [39]. Overall, blockchain technology offers phenomenal services across the energy society, as it promotes sustainability and decarbonisation with better management of RES. These services can be summarised as below:

1. Data Security: Blockchain utilises cryptographic techniques and public key signatures to secure the transactions, ensures data confidentiality and respect privacy [81]. It also provide identity management services [81].

2. Transparency: traceability of the transactions is possible with this technology as it keeps the track record of all the transactions into immutable and transparent ledgers which provide access to transparent data for different purposes like auditing and compliance.

3. Local energy markets: Blockchain supports peer to peer energy trading by enabling local and customer-oriented marketplaces [82] which may disrupt current market operations and greatly improves the economics of all players involved in trading thus promoting more p2p local energy trading. Sales or purchases practises under this platform changes flexibly depending on the needs and preferences of the participants.

4. Billing: This technology may automate billing operations for the participants

using smart contracts and incorporating smart metering infrastructure and this will directly benefit the utility companies [83].

5. Network Management: Blockchain could optimise grid operations and greatly assist in overall grid management by offering phenomenal automated services e.g. automated transaction settlements, billing, identity and asset management etc. Thus it reduces the transaction costs, increases revenues and saves the network from expensive upgrades.

6. Scalability: Decentralised distributed ledger technology(DLT) provides resilience, energy efficiency and better scalability with high performance speed using one of the best consensus algorithms designed for it.

7. Small energy footprint: DLTs promotes local decision making and introduces distributed control which can significantly reduce the requirement of computational resources thus resulting into more energy efficient future power systems.

Observing these services, blockchain distributed ledger technology could bring disruption to the existing business models and energy companies. Ongoing research activities, pilot projects and trails will reveal its full potential and adaptability in the commercial stream.

However it is challenging to completely transform the whole structure of existing power system network in the short time. Therefore, most of the existing running blockchain projects are focused on one of the different areas of the power systems e.g. there are several use cases of blockchain in energy sector such as wholesale energy trading, blockchain trading for utilities and energy system stakeholders, P2P trading in community projects and microgrids, blockchain technologies for renewable or carbon certificates, blockchain for grid management [13].

However this thesis will be focusing on one of its use case i.e. energy trading support for small generators and end-consumers by peer to peer blockchain based platform. The platform proposes design architectures both for existing regulated market structures and for deregulated market structures [25]. However later is still a

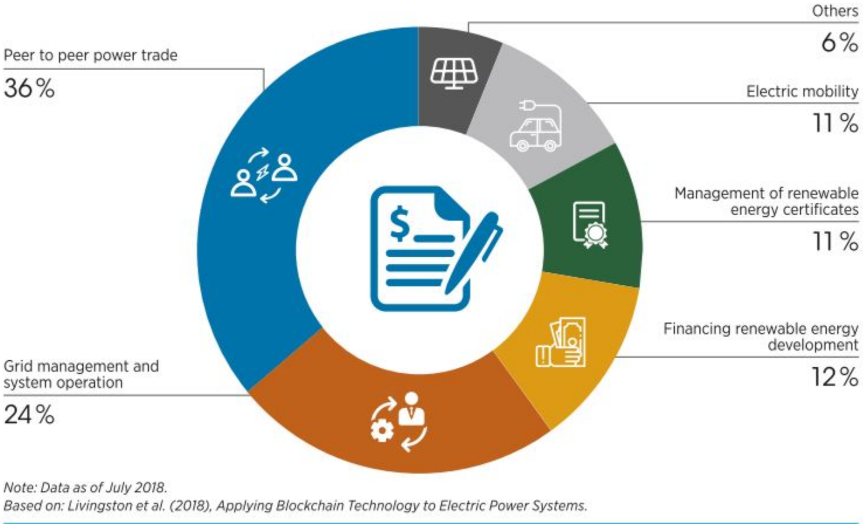


Figure 4-1: Blockchain Applications in Energy Sector [12]

premature concept and is a subject of current research studies. Therefore, the former will be the topic of further discussion.

4.2.1 Role of TSOs, DSOs

In this context, it is very important to understand the role of DSO/TSO in the proposed P2P architecture because they hold the physical infrastructure and are responsible for handling grid operations to maintain grid stability. DSO/TSO can support the P2P trading platform by providing and managing the access to the power grid for energy exchanges but they are not required to centrally manage the energy transactions [13]. They are responsible for assuring that a P2P energy trade can actually take place over the network, provided the physical constraints. Using the information from P2P transactions record on blockchain, they can manage the power flows through the network and also the capacity. With the integration of Artificial Intelligence and Machine Learning tools, in future it would be possible for the system operators to receive forecast about the energy supply and demand of the users hence, it could make early adjustments in the system before even the trade starts. P2P transactions costs also account for the DSO and TSO services therefore grid charges are inclusive in the prices or tariffs set for these transactions.

4.3 Core technologies

Digitalisation of Energy and IoT

Emergence of IoT platforms and development of ICT have open doors for new and exciting applications of blockchain technology [84]. By 2020, it is estimated that around 20 billion of smart devices would join the internet world [81]. In the field of energy, an increasing number of smart meters and ICT equipments are being installed in order to facilitate the power system with advanced metering infrastructure [85]. Blockchain based P2P trading platform allows machine to machine communication between the smart devices enabling data exchanges across the network. Smart meters integrated with the blockchain can facilitate to record and track the data (about energy produced and consumed at each time interval with the location) on the temper-proof ledger. Moreover programmable smart devices using artificial intelligence and machine learning capabilities, are also able to perform more functionalities in the future. For example, autonomous trading agent could decide bidding strategies based on user preferences, weather forecast, battery activity, prediction of the energy production and consumption by user behavior. Some companies [86] [87] are designing and producing smart devices which have extra functionalities and capabilities e.g. Verv has developed hardware product VHH which is capable of utlra high resolution electricity sampling, 5 millions faster than a smart meter [26]. VHH connects smart home devices to the cloud and offers controllability to user via mobile application featuring home automation, energy conservation and cost reduction [26]. Further research and activities are in progress to reveal more capabilities of IoT and blockchain merger.

Cloud and Edge Computing

Emerging cloud and edge computing paradigm shows the potential capabilities for transactive control in the local energy market, offering distributed computing and storage services [71]. Blockchain, cloud and edge computing inter-operates to provide infrastructure support for the implementation of the blockchain applications in different areas. This enables autonomous contract execution for network edge users and reduces the requirement of trusted third party platform. Cloud computing is an integration of computer and network technology therefore, it combines the services such as distributed computing, network storage and load balancing. Cloud and edge computing provides distributed cloud framework to facilitate network edge users, which is appealing to the blockchain decentralised applications [88] [89].

Big Data and artificial intelligence

Automated decision-making, big data management, data acquisition and market prediction are being the emerging innovative demands of the current blockchain applications since the Big Data, Machine Learning and AI technologies are introduced. These technologies have the capabilities to enhance the features of the blockchain to a next level. Autonomous cars and drones are the one of the wonders that can be expected with integration of blockchain smart contracts technology and AI capabilities, providing behaviour management infrastructure. Whereas, in the energy sector, their interoperability could enable automated decision-making for energy trading by prediction of energy production and consumption, weather forecast, prediction of battery conditions and user behaviour. Since, the increasing volume of data on blockchain with the induction of IoT driven smart devices, can not be handled with the traditional data management and analysis services. Therefore, it requires the big data solutions which uses advanced computing, data mining and machine learning algorithms [90] for handling big data i.e. data acquisition, processing, analysis and maintenance. Thus, numerous exciting, innovative and interesting blockchain-based applications might be seen in the coming future, with the adaptation of big data and AI technologies.

4.4 Current Status and Initiatives

When the blockchain technology and the world of energy intersects, several application categories emerges. Among these categories are: P2P transactions, grid management and system operation, financing renewable energy development, management of

RECs and certification of origin, and electric mobility. Since, this thesis is intended to research the blockchain application for P2P energy trading, therefore this area will be explored in the following. For the last few years, several startups and pilot projects have been carried out on the development of P2P energy trading platforms using blockchain decentralised architecture, showing promising results for the future power systems.

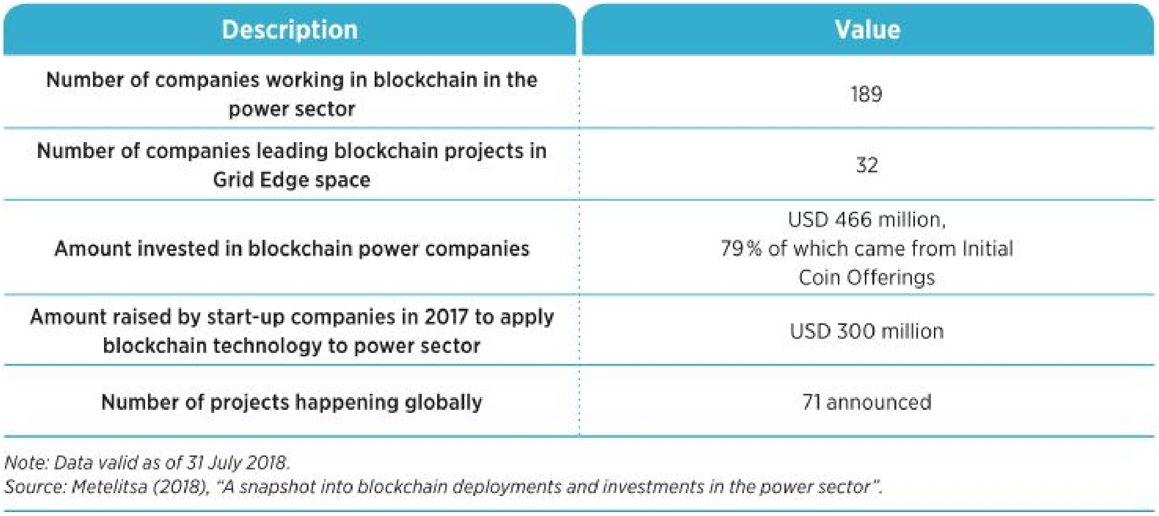
Power Ledger, an Australian based startup, developed interoperable energy trading platform using ethereum blockchain that supports a growing number of energy applications such as neo retailer, whole sale market settlements, distributed market management, autonomous asset management, electrical vehicles however, the most mature developed application is P2P energy trading marketplace between local prosumers and consumers. Power ledger presents two models, retail model for existing regulated market structure and direct peer to peer model for deregulated market structures; [25]. Moreover, it has also introduced a dual token ecosystem for facilitating energy trading.

LO3 in partnership with Transactive Grid developed a community microgrid in NY,USA. The project provides technical infrastructure for the local electricity market based on private blockchain using Tendermint protocol [24]. The company introduced transactive grid smart meters to transmit energy data to blockchain accounts of users. LO3 was the first pilot project to achieve the first P2P blockchain transaction between a prosumer and his neighbour. The company is intended to announce more pilot projects in future.

Grid+ developed a blockchain platform for energy trading using ethereum that provide producers and consumers direct access to the electricity market. Grid+ agent has been designed to provide services of retail supplier by making automated decision for trading for its user [27].

Verv trading platform, a UK based pilot project which has introduced smart devices which are able to provide high resolution of energy data and very high speed performance than other smart meters. The company has developed Verv Home Hub (VHH) using AI and machine learning tools that connects smart home devices to the cloud and offers controllability to user via mobile application featuring home automation, energy conservation and cost reduction. Based on ethereum smart contract technology, Verv has proposed a market model and ecosystem for regulated systems where local aggregators could enable prosumers and consumers to transact using blockchain platform. According to the Verv, VLUX tokens will be used for trading and will be facilitated by local aggregators [26].

These are just few prominent projects mentioned here but actually there is a series of companies, consortium, foundations and working groups which are being involved in the research and development for blockchain based energy applications. The synthesis report 2019 by IRENA [12] as shown in figure 4-2 provides very good and latest statistics of all the blockchain projects development in energy field.

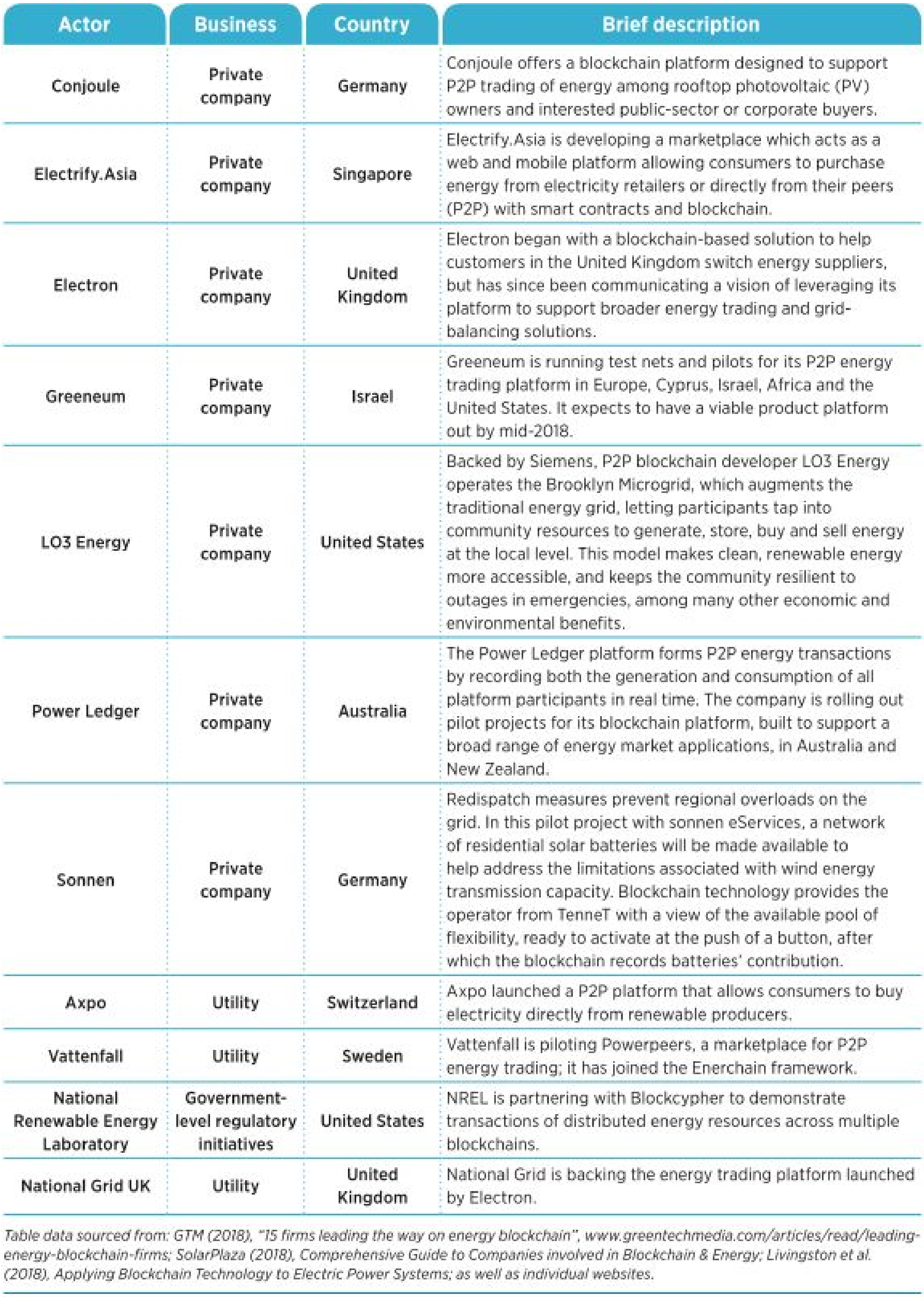


Description	Value
Number of companies working in blockchain in the power sector	189
Number of companies leading blockchain projects in Grid Edge space	32
Amount invested in blockchain power companies	USD 466 million, 79% of which came from Initial Coin Offerings
Amount raised by start-up companies in 2017 to apply blockchain technology to power sector	USD 300 million
Number of projects happening globally	71 announced

Note: Data valid as of 31 July 2018.
Source: Metelitsa (2018), "A snapshot into blockchain deployments and investments in the power sector".

Figure 4-2: Statistics of Blockchain Developments in Power [12] Sector

Moreover, the details of around 140 more projects including their field area, platform, consensus algorithms and locations have been tabulated in a survey [13]. According to the IRENA report, based on analysis of 150 leading pilot project and companies, as of september 2018 it was found that over 46% of these energy blockchain startups are founded in Europe. Whereas USA, Germany and Netherlands are the three top countries in this field. Moreover, around 50% of the projects are using ethereum platform for development.



Actor	Business	Country	Brief description
Conjoule	Private company	Germany	Conjoule offers a blockchain platform designed to support P2P trading of energy among rooftop photovoltaic (PV) owners and interested public-sector or corporate buyers.
Electrify.Asia	Private company	Singapore	Electrify.Asia is developing a marketplace which acts as a web and mobile platform allowing consumers to purchase energy from electricity retailers or directly from their peers (P2P) with smart contracts and blockchain.
Electron	Private company	United Kingdom	Electron began with a blockchain-based solution to help customers in the United Kingdom switch energy suppliers, but has since been communicating a vision of leveraging its platform to support broader energy trading and grid-balancing solutions.
Greeneum	Private company	Israel	Greeneum is running test nets and pilots for its P2P energy trading platform in Europe, Cyprus, Israel, Africa and the United States. It expects to have a viable product platform out by mid-2018.
LO3 Energy	Private company	United States	Backed by Siemens, P2P blockchain developer LO3 Energy operates the Brooklyn Microgrid, which augments the traditional energy grid, letting participants tap into community resources to generate, store, buy and sell energy at the local level. This model makes clean, renewable energy more accessible, and keeps the community resilient to outages in emergencies, among many other economic and environmental benefits.
Power Ledger	Private company	Australia	The Power Ledger platform forms P2P energy transactions by recording both the generation and consumption of all platform participants in real time. The company is rolling out pilot projects for its blockchain platform, built to support a broad range of energy market applications, in Australia and New Zealand.
Sonnen	Private company	Germany	Redispatch measures prevent regional overloads on the grid. In this pilot project with sonnen eServices, a network of residential solar batteries will be made available to help address the limitations associated with wind energy transmission capacity. Blockchain technology provides the operator from TenneT with a view of the available pool of flexibility, ready to activate at the push of a button, after which the blockchain records batteries' contribution.
Axpo	Utility	Switzerland	Axpo launched a P2P platform that allows consumers to buy electricity directly from renewable producers.
Vattenfall	Utility	Sweden	Vattenfall is piloting Powerpeers, a marketplace for P2P energy trading; it has joined the Enerchain framework.
National Renewable Energy Laboratory	Government-level regulatory initiatives	United States	NREL is partnering with Blockcypher to demonstrate transactions of distributed energy resources across multiple blockchains.
National Grid UK	Utility	United Kingdom	National Grid is backing the energy trading platform launched by Electron.

Table data sourced from: GTM (2018), "15 firms leading the way on energy blockchain", www.greentechmedia.com/articles/read/leading-energy-blockchain-firms; SolarPlaza (2018), Comprehensive Guide to Companies involved in Blockchain & Energy; Livingston et al. (2018), Applying Blockchain Technology to Electric Power Systems; as well as individual websites.

Figure 4-3: Example of some prominent initiatives in the field of blockchain based peer to peer electricity trading [12]

4.4.1 Platforms

In order to explore more potential use cases of blockchain in energy sector, several collaborative platforms have been established by different organisations. One of the biggest framework and blockchain platform founded is Ethereum as discussed in detail in the previous chapter. Ethereum enables the development of decentralised blockchain applications. Moreover, Grid Singularity in association with rocky mountain institute et al, founded Energy Web Foundation(EWF) which aims to accelerate the use of blockchain technology across the energy space to introduce decentralized, democratized, decarbonised and resilient energy system. EWF provides a blockchain based software infrastructure named as Energy Web Chain, providing an environment to develop, test and deploy energy blockchain applications. The platform is based on Ethereum and uses proof of authority(PoA) consensus algorithm called Aura [91], developed by parity ethereum client technologies. It has launched its public test network called Tobalaba which offers 3s block generation time to achieve higher throughput. Energy web chain using PoA mechanism improves ethereum performance to 30 times. It is aimed to provide a governance structure that balances advantages of decentralization with regulatory oversight and promotes innovation [91].

Hyper Ledger hosted by Linux Foundation, is a global, open source collaborative effort in order to bring advancements in the blockchain technologies. It provides distributed ledger frameworks and community driven infrastructure backed by business technical governance to develop, test and deploy blockchain use cases. In other words, hyperledger consists of communities based on software developers who are jointly building blockchain frameworks and platforms. Hyperledger is developing several consensus algorithms and frameworks that provides features and functions to help the development of blockchain solutions for different domains spanning banking, financial services, health care, supply chain management, IT and extended to more [92].

There are other collaborative platforms and ecosystems, as depicted in Fig.4-4 that are evolving to support the development of exciting new blockchain applications

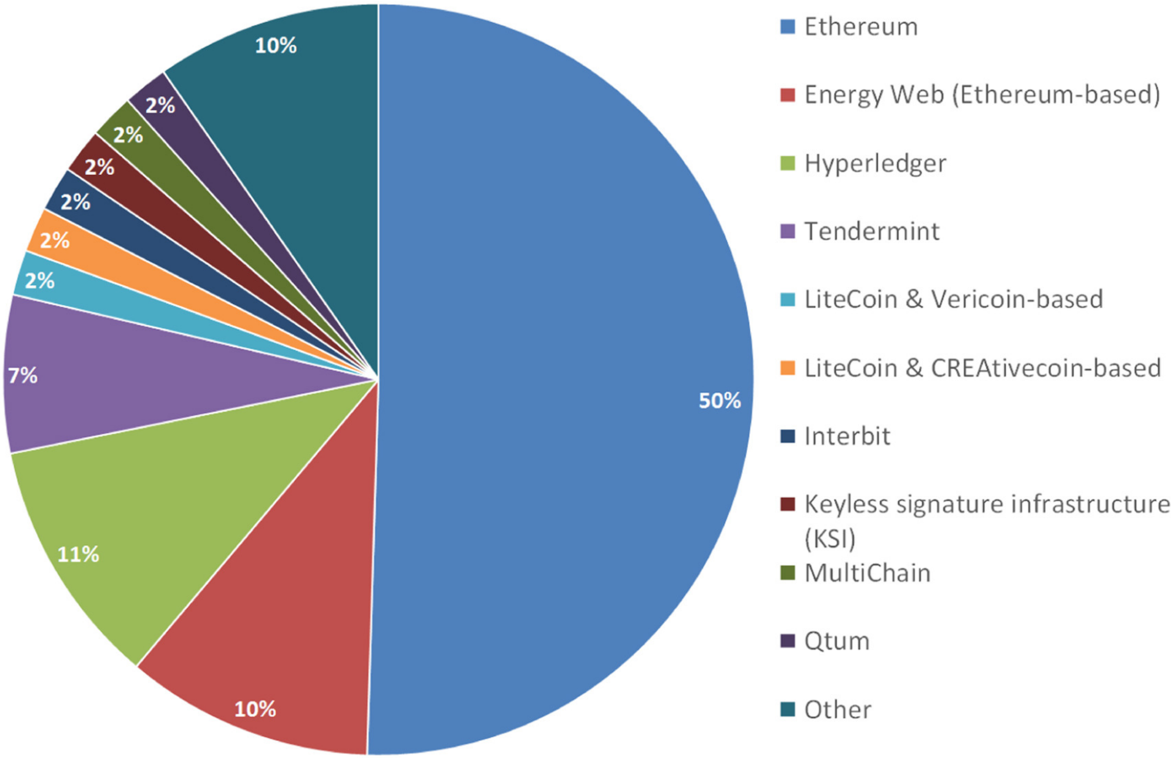


Figure 4-4: Blockchain use cases in the energy sector according to blockchain platform used [13]

and where the developers around the world gathers to bring innovative ideas and develop them into realised application benefiting the whole energy society.

The review of these blockchain based research initiatives, pilot projects and startups, demonstrate the true potential of the blockchain technology and promising use cases of it in the energy industry. Although, there are numerous projects, research activities and publications in this area however, they still do not provide the technical details and explanation about their implementation work. Therefore it is challenging to get the full knowledge about the development of these applications. However, this thesis aims to provide the missing pieces and intended to provide detailed information about the software and hardware tools, and also about designing, testing and deployment of the basic P2P model for local energy trading.

4.5 Challenges

Despite, the blockchain appears as a promising and revolutionary application for P2P energy trading however, it also put forth some challenges which need some consideration. The integration of IoT systems introduces smart devices which are designed to interact with the smart contract and transmit energy data i.e. consumption or production by users, which is stored into the distributed ledgers. This significantly raises security and privacy concerns since the public blockchains are accessible for all the parties and provides traceability and transparency to the records history. Due to these concerns, players might show resistance to participate in this platform. Therefore a novel solution is required in order to preserve anonymity and privacy of the users so that their energy usage data could not be traceable by other individual users. A solution is required which also complies with the regional legal privacy requirements such as GDPR. In this scenario, permissioned blockchain seems to be a potential solution which restricts everyone from access and allows only authorised individuals to access the data for useful purposes e.g auditing and compliance.

Another main concern is the ever-expanding volume of the data because of the introduction of smart meter data from each user and also growing number of users joining this platform. The storage and management of this huge data can not be handled with the existing infrastructure capacity. In this domain, innovative big data framework and tools can be adopted which may facilitate the handling of huge data using services such big data management, big data analysis and data mining. However, there are still more challenges such as grid defection and under-utilisation of network assets, pertaining to P2P local energy marketplaces [13].

Evidently, this field i.e. blockchain based P2P energy trading is still immature to be adapted into the mainstream because it is in early stages of development but further R&D work will unfold its full potential and adaptability at a commercial scale.

Chapter 5

Implementation

It has been observed from an extensive literature analysis that previous projects and models do not provide the detailed technical explanation required to understand the implementation details. Therefore, this thesis is intended to provide necessary technical details to develop a sound background and understanding of the implementation of proposed model. This chapter will follow the same.

5.1 Physical and Virtual network

A peer to peer(P2P) distributed energy network is composed of two layers. One layer is physical energy network and second layer is virtual energy trading network. Physical network layer includes distribution grid which is responsible for the physical transfer of energy between the peers. This could be be a traditional distributed grid network operated by independent system operator (ISO) or a separate microgrid connected to a traditional grid. Virtual energy trading platform provides the technical infrastructure i.e blockchain based architecture for local energy market where all kinds of data transfer takes place e.g. electricity production, consumption and demand data of peers are transferred to virtual layer by smart meters over a communication network [93]. All buy and sell offers are created in virtual layer where the offers are matched and accepted, payments are executed between peers and the energy exchange takes place over physical layer. Financial transactions are executed in virtual layer and they actually have no effect on physical energy transfer. Payments are made by consumers to prosumers for exporting their renewable energy to the distribution grid.

This study is intended to provide technical implementation details of a simple demonstration of how this energy trade takes place between the peers. In order to start implementation, it is important to signify the roles of participants in this peer to peer energy trade network.

- Peers: In this context, peers can be defined as the players who are buying or selling the excess of produced renewable energy in neighbourhood i.e. within the network. Peers are categorized as:

    1. Consumer: a participant who always consumes electricity.
    2. Prosumer: a participant who has some renewable energy generation system and both consumes and produces electricity.

- Local Aggregator: Large P2P energy trading network is split into communities where each community have its own local aggregator who serves as a broker function for its local trading community network which enables peers within their network to trade electricity. Local aggregator purchases tokens from public exchange and sell tokens locally to the participants on request, with which they trade electricity on the platform.

5.2 Scenario/IDEA

For this demonstration, a simple scenario has been build based on regulated system assuming Peer A and Peer B are the registered participants on our energy-trade platform. A mobile application service has been provided to the users for ease of accessibility to execute trading.

1. Peer A wants to sell his surplus produced energy. He'll use our energy-trade platform and will make an offer via mobile application provided by the platform.

2. Peer B is interested in the offer and wants to buy energy so he'll pick the offer via mobile application.

3. Peer B pays local aggregator the amount as mentioned in offer.

4. Local aggregator asks Peer A to start exporting energy and Peer B starts consuming energy.

5. Local Aggregator investigates the proof of delivery(PoD) by means of smart meter data on both ends.

6. Once PoD is confirmed, local aggregator pays Peer A, for the energy he sold.

5.3 Development tools

It was a big challenge to identify the exact tools required for the implementation of the presented idea. During the research phase, different tools were explored and tried which followed many revisions. Eventually, the following hardware and software tools were opted.

5.3.1 Hardware

1. **Raspberry Pi 3 Model B+** (in Fig. 5-1) is a single-board computer which is used as smart meter installed at the participant's house. At first, Arduino microcontroller was chosen because of its compact size and specific functionalities as compared to Raspberry Pi but it had some issues with Web3 library which is required for communicating with the smart contracts.

2. **LEDs** are used for indicating trading session. Whereas, 8x8 RGB LED matrix of Sense HAT that is an add-on board of Rasberry pi, is used to display the status of the energy transaction.

3. **Rotary potentiometers** emulate the behaviour of participant's energy consumption and production, which are varied manually for displaying the energy

change.

4. **MCP3008 ADC** (Analog to Digital converter) chip is used for reading the data from potentiometer i.e. produced or consumed energy and send the digital converted value to the smart meter.

5. **Local aggregator** services are programmed in a server which keeps the data record of the users and their smart meters. Moreover, other services include token exchanges, payments settlements and proof of delivery operation.

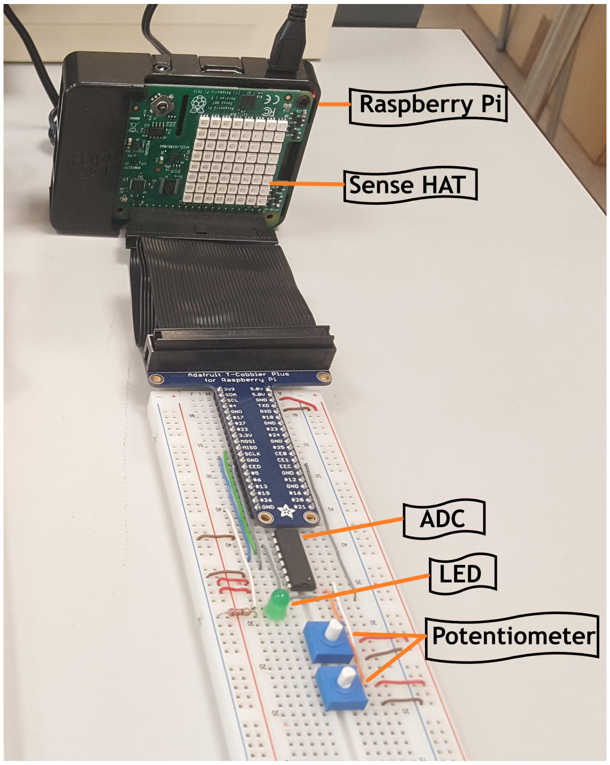


Figure 5-1: Hardware SETUP

5.3.2 Software

1. **Energy Web Foundation(EWF)-Tobalaba Test Network** is used to build and test the smart contract. EWF provides Energy-Web UI (user interface), a frontend which has been used for creating accounts, writing smart contract, deploying and testing it on Ethereum Tobalaba network.

2. **SQLite** database engine was used for the creation of smart meters and users database, and for making data queries to the database such as insert, update or select data.

3. **Node-RED** flow-based development tool for visual programming is used for implementing the platform services i.e. local aggregator functionalities, interacting with the smart contract, smart meter communication with the data server. Moreover, Node-red is also used as a backend for Ionic application

4. **Ionic** which is an open-source front-end web application framework, is used for building Energy Trade mobile application using **Angular** framework.

5. **Web3** Ethereum JavaScript API is used to interact with the Ethereum blockchain network. This library allows to retrieve user accounts, interact with smart contracts, send transactions and more.

5.4 Methodology

The first research challenge was to create the smart contract to implement different functionalities of the proposed P2P energy trade design model. Based on thorough research and the project's technical requirements, Energy Web Foundation (EWF) ecosystem has been chosen for the development of our smart contract on Ethereum blockchain.

EWF is the world's largest energy blockchain ecosystem structured for energy sectors regulatory, operational and market needs [91]. This platform provides open source frameworks equipped with development tools for developing blockchain based commercial decentralised applications such as the implementation of business logic functions in a smart contract.

In order to start implementation, Energy Web Client UI (user interface) was installed from EWF platform. Energy Web Client UI is a user interface desktop application for connecting the peers in the blockchain network, creating accounts, sending transactions and for deploying and interacting with smart contracts. This client is based on parity ethereum client therefore it provides development tools for the creation of the smart contracts, testing and deployment on the Ethereum platform.

5.4.1 Accounts Creation

With Energy Web UI, parity ethereum wallet accounts are created for the registered users and the local aggregator. The biggest advantage of these environments is that the fake tokens are issued to the developer enabling him to transact over the blockchain for development procedures such as testing and deployment of smart contracts. EWF redirects to Energy Web Tobalaba testnet faucet where users with their public keys can receive free test tokens.

5.4.2 Smart Contracts Creation

Energy Web UI provides the option to develop smart contracts. In order to implement the proposed secenerio/idea as discussed earlier, we designed main functions of our smart contract using Solidity, which are mentioned below:

- `Add Offer`: This function is designed to facilitate peers basically prosumers to create their offer by adding some details to it i.e. how much energy a prosumer is intended to sell? At how much price? All these details are saved by this function. The structure of an offer is depicted in table 5.1.

Table 5.1: Energy Trade Offer

Structure of an Offer		
Size	Arguments	Details
32 bytes	ID	offer ID
20 bytes	seller	seller address
32 bytes	energy	amount of electricity for sale
32 bytes	price	price of electricity for sale
32 bytes	timeOffered	time when offer is added

- `Pick Offer`: When a peer i.e. a consumer in this case, is interested in any offer. He invokes this function in order to confirm his choice and hold this offer

- `confirmP2L_Tx`: This function is entitled to check the status of transaction made by the consumer to the local aggregator. It confirms if the consumer has paid for the offer he accepted.

- `PoD`: Local aggregator invokes this function to confirm the delivery of energy by the prosumer. It triggers the further process.

- `confirmL2P_Tx`: This function is designed to confirm the payment made to prosumer by local aggregator and to complete successfully the peer to peer energy trade.

Developed Artifact

Based on the above mentioned functions, smart contract was developed. The deployment of the smart contract cost some gas units based on the logic operations used in the program.

The designing process took a significant amount of work. A lot of revisions and improvements were made during the design process. The final source code is available in Appendix A.

5.4.3 Design Model

The central idea behind the design was to create a simple demo of a local energy trading community within a regulated system. There are four main driving components of the proposed platform which enable local energy transactions among peers that are blockchain based smart contract, local aggregator, smart meters and mobile application service. The smart contract is designed with some functionalities as earlier discussed in detail, to provide local energy market to the participants (prosumers and consumers) where they can make energy offers or buy energy. Moreover, it validates the payments and provide energy transactions storage on the Ethereum blockchain. Local aggregator (L.A) is appointed to provide transactive management to the platform. It provides all the basic software and communication networking components for the exchange of information required to execute an energy transaction. Smart

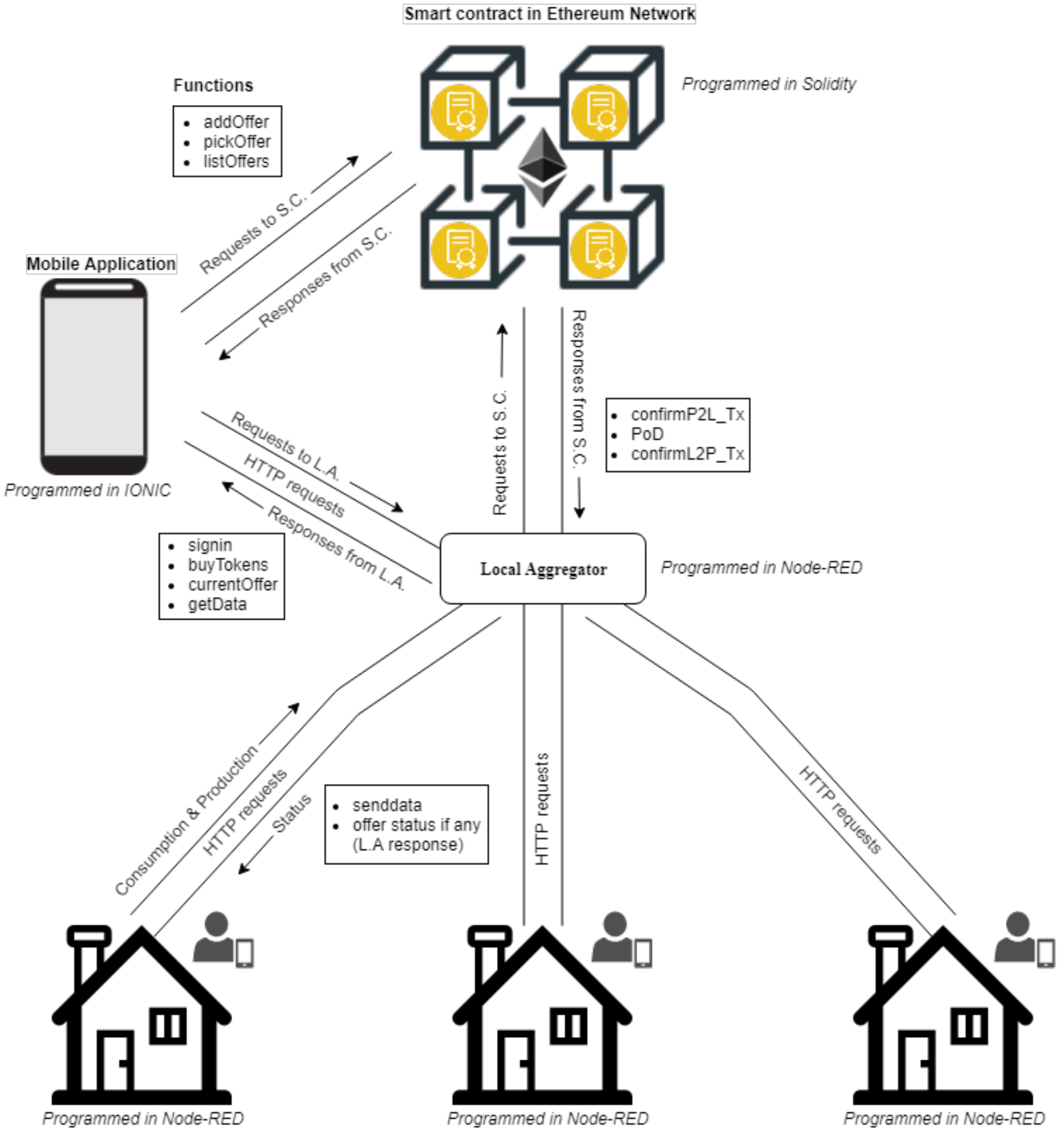


Figure 5-2: Design Model of Blockchain-Based P2P Energy Trading using IoT Devices

meters are installed at each participant's house which are periodically measuring and sending the consumption and production data to the L.A server and saved into the database.

Mobile application service is developed to provide users an access to the platform services. It provides all the functionalities of the platform connecting users to the smart contract and local aggregator. Each component collaborate with other component to provide certain functionalities that are illustrated in Fig. 5-2 such as mobile application enables participants to sign in and buy tokens which are facilitated by L.A server. Moreover, further explanation for each component and functions are provided in their subsequent sections whereas the designed smart contract functions have already been explicitly defined in earlier section.

5.4.4 Advanced Metering

Smart meters are modeled as Raspberry Pi's which are programmed using node-red visual programming to provide advanced metering services. Moreover, the energy production and consumption by the participants are also emulated using potentiometers which are varied to represent the changes in produced and consumed energy. Furthermore, the smart meters of the participants are also registered with the platform and each one is identified with its ID. These smart meters periodically send their measured energy data to the local aggregator server every second.

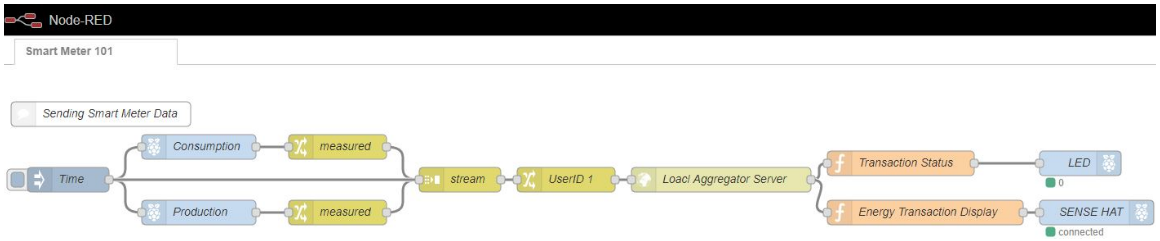


Figure 5-3: Smart Meter Functioning

Fig.5-3 shows the program flow of the smart meter where the `time` named node is the inject node which initiates the flow and is set to one second. The information including measured values of produced and consumed energy along with the user ID is post via http request to the *senddata* URL of L.A server specified for smart meter data. In response, the L.A returns the transaction status which is visualised with an indicator LED. Moreover, the transacted energy information if any, is displayed on SENSE HAT for the user.

5.4.5 Local Aggregator Server

Local aggregator services are programmed on a server using the node red visual programming. All the designed program flows for providing these services are discussed step wise below.

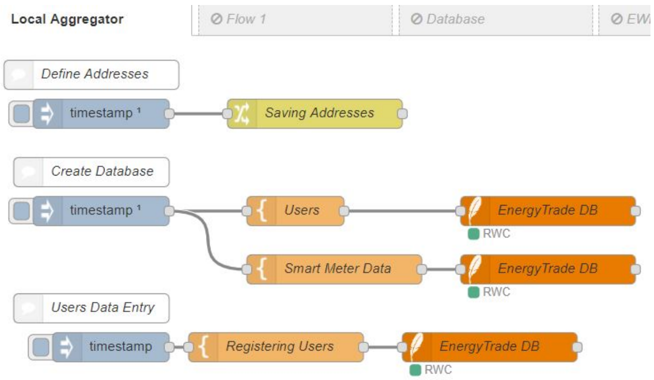


Figure 5-4: Data Registration

As shown in Fig.5-4 firstly, all the required addresses such as smart contract address, local aggregator account public key and private key, are defined in the L.A server to interact with the smart contract on the blockchain. Then, all the users along with the smart meters installed in their premises, are registered on the platform database (as represented by *EnergyTrade DB* node) created, managed and accessed by using SQLite functionalities.

Fig.5-5 depicts the program flow to provide sign in functionality. When the user signs in using mobile application service of the platform, his credentials are post via http request to the *signin* URL of the L.A server. The validity of the credentials is checked against the record of registered users and if the credentials are wrong, the error message is sent in response to the *signin* request. In case of the valid details,

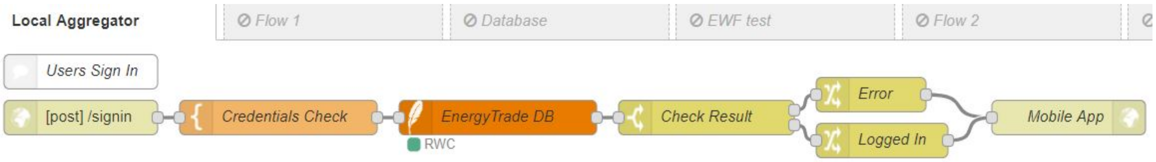


Figure 5-5: Sign in Functionality

user is given access to the mobile application services.

In Fig.5-6 L.A receives the smart meter data of the users which is identified with the user ID and saved into the respective smart meter database, against that user ID. Moreover, if the corresponding user has an energy transaction in process, then L.A identifies consumer or producer from the user ID and sends the respective transacted energy info in response to the smart meter. Moreover, when the user requests the meter data for monitoring via mobile app, it posts http request along with the user id to *getdata* URL of the L.A server which extracts the corresponding smart meter data from the database and sends it in response to the mobile app request. Thus, the mobile app displays the smart meter data to the user.

The *currentoffer* functionality as depicted in Fig.5-7 provides the details of the energy transaction in process, made by the user. Http request is made to *currentoffer* URL when the user prompts this field and in response L.A firstly checks if there is any transaction of this user in process. Based on the validity respective details are responded which are then displayed by the mobile application.

Fig.5-8 provides the L.A program flows designed to perform PoD functionalities. When the user picks an energy offer and makes the payment to the local aggregator,

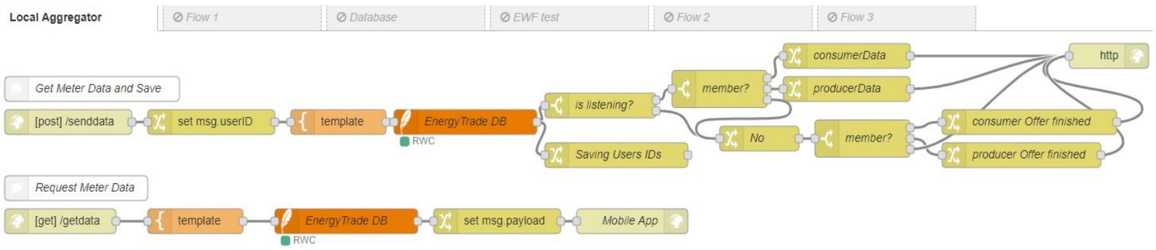


Figure 5-6: Smart meter data storage and monitoring

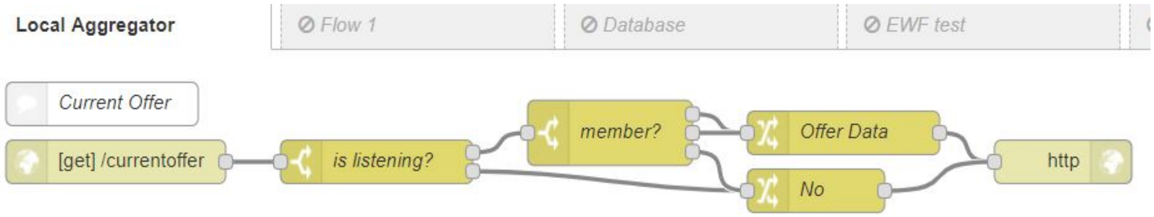


Figure 5-7: Current Offer functionality

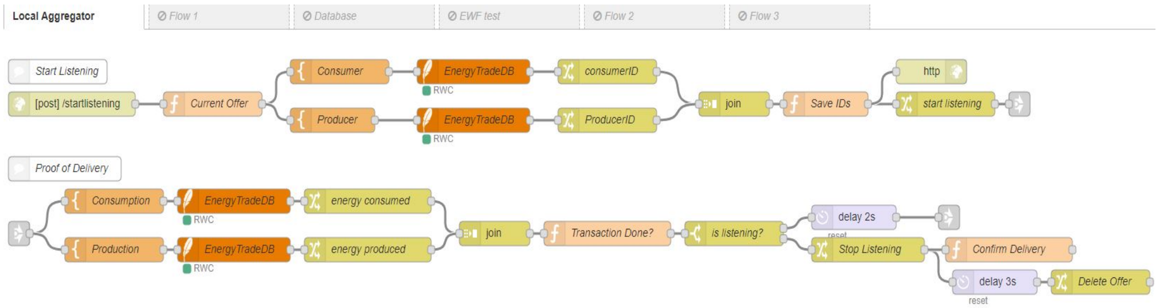


Figure 5-8: Proof of Delivery functionality

the smart contract function `confirmP2L_Tx` confirms the payment transfer and invokes *startlistening* URL. Using *Offer ID* provided by the smart contract, L.A extracts the consumer and prosumer IDs from the database, and initiates the PoD process. In this process, L.A keeps checking the smart meter data of both prosumer and consumer from the database to verify that the targeted energy has been delivered. Once L.A confirms the delivery to the smart contract and finally makes the payment to prosumer which is confirmed by the smart contract. Once the energy transaction is processed, the offer is deleted from the *current offer* list.

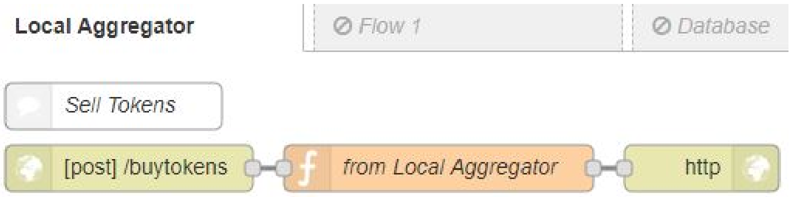


Figure 5-9: Broker Function

L.A provides a broker function in the local energy trading community and enables participants to trade electricity on the platform. L.A facilitates tokens to the participants in order to use the services of the platform and trade energy over the network. Platform sets the value of the token, in this platform 1 token = 500 milli ether for the demonstration purposes. When the user requests tokens, mobile application service posts http request to the *`buytoken`* URL of the L.A server which transacts tokens with the users in exchange of ethers on the Ethereum blockchain.

5.4.6 Mobile Application Development

The front end of the platform is provided by the mobile application which entertains the users with the platform services. Some of the functionalities of this application have been already discussed in earlier section. Moreover, panel views of the application have been provided in Fig.5-10.

Panel ⓐ is the login page where users enter the credentials. In the back end, mobile application service makes *`signin`* http request to the L.A server as discussed earlier. In the case of valid credentials, user is redirected to the menu page.

Panel ⓑ in Fig. 5-10 displays the menu of all the services provided by the platform.

Panel ⓒ shows the profile page, where the details of the user such as name, account address and tokens available are displayed. This provide users to keep check and balance of the account.

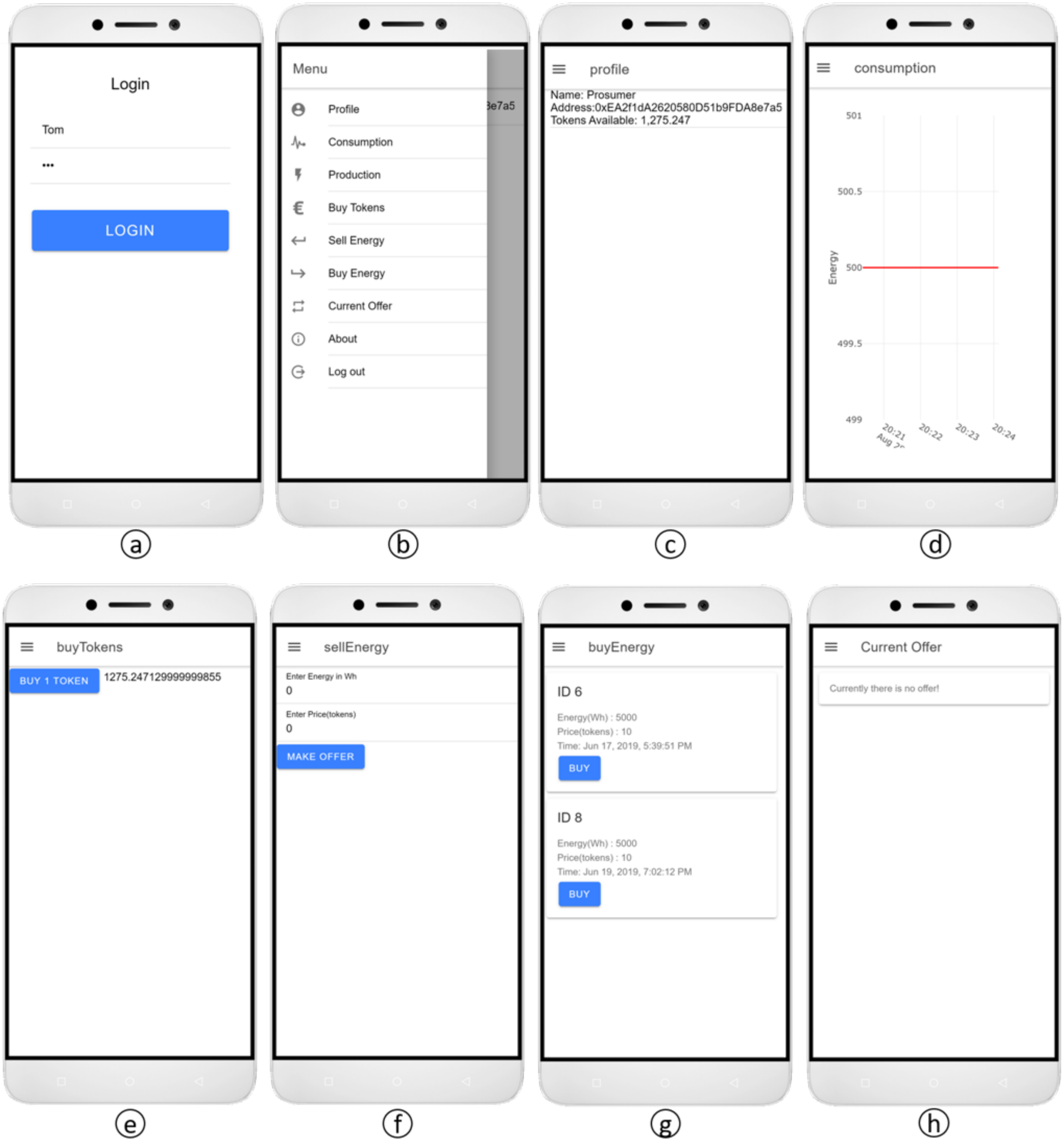
Panel ⓓ provides the user with the real time monitoring of the energy consumption and also the same for the energy production. Mobile application service makes *`getdata`* http request to L.A server which returns the reading of respective smart meter as earlier discussed.

Panel ⓔ provides the page where user can buy tokens from L.A. The back end functioning have already been covered in earlier section.

Panel ⓕ is the page which allows users to make an energy offer and invokes the `Add Offer` function of the smart contract passing energy and price data as arguments with the details of the user and time.

Panel ⓖ represents the lists of the available offers to the user with offer ID, energy, price and time posted details. In the back-end, the service calls the `list offer` function of the smart contract which returns all the available energy offers. When the user picks the offer, the `Pick Offer` function of smart contract is invoked by the service and the details of the user are passed as arguments. The offer is then removed from the list and energy price is transacted from user account to L.A account.

Panel ⓗ is the page which displays the picked energy offer if there is any, which is in the transaction process.



Tom

•••

Name: Prosumer
Address:0xEA2f1dA2620580D51b9FDA8e7a5
Tokens Available: 1,275.247

1275.247129999999855

Enter Energy in Wh
0

Enter Price(tokens)
0

ID 6

Energy(Wh) : 5000
Price(tokens) : 10
Time: Jun 17, 2019, 5:39:51 PM

ID 8

Energy(Wh) : 5000
Price(tokens) : 10
Time: Jun 19, 2019, 7:02:12 PM

Currently there is no offer!

Figure 5-10: Energy Trade Mobile Application Panels

Chapter 6

Discussion and Conclusion

6.1 Blockchain Application for P2P Energy Transactions

As reviewed in this thesis, the promising characteristics of the blockchain decentralised ledger technology show its viability to meet the prevailing challenges to existing power systems. Blockchain offers innovative P2P energy trading platforms that enable beneficial energy exchanges among participants which represents evolution for future smart grids. This paradigm shift towards decentralised P2P local energy trading can immensely reduce the transmission losses and also defer expensive upgrades in the network. Contrary to the centralised architectures, the blockchain distributed ledger eliminates the third party involvement ensuring integrity and security of the system. Blockchain uses automated smart contracts technology which improves cyber-security and optimises the energy processes which can significantly reduce the transaction costs. Along with IoT integration such as advanced metering infrastructure, this decentralised architecture can offer more flexible and efficient energy markets which in turn add resiliency to the power system network. Overall, blockchain technology offers phenomenal services across the energy society, as it promotes sustainability and decarbonisation with better management of RES.

Despite, the blockchain appears as a promising and revolutionary application for

P2P energy trading, it also put forth some challenges which need some consideration. For example, the integration of IoT systems introduces smart devices which raises issues such as privacy leakage and ever-expanding volume of the data storage and management. Grid defection and under-utilisation of network assets, are other more issues pertaining to P2P local energy marketplaces. Moreover, research challenges such as regulation and governance, also exists. Nevertheless, blockchain is a scalable platform and also a fast-moving area of research and development because in a short time span, a great advancement and development have been witnessed in this field. There are many research initiatives, collaborative platforms and ecosystems, that are being focused on the development and improvements of energy blockchain applications. Additional research activities e.g possible integration of AI, cloud computing and machine learning algorithms with blockchain may help in unlocking the full disruptive potential of this technology which makes it suitable for market reliability and to be deployed at a large scale.

Several research initiatives, companies and collaborations have been focused on the development of these applications to improve overall efficiency and economy of the existing energy systems

6.2 Contributions

A simple peer to peer energy trade model based on the Ethereum Blockchain framework, is designed and successfully implemented based on in-depth research and literature review, which is a big achievement. This thesis provides a valuable documentation because a systematic approach has been acquired to provide deep conceptual understanding of the blockchain technology and its useful application in the energy sector i.e. P2P energy trading. Moreover, this thesis provides all the necessary technical details and steps required to build the simple model of blockchain application for energy transactions. Furthermore, a mobile application has been developed to provide user friendly interface for the participants to use the services offered by the designed model. The source code of the developed smart contract with its function definitions, has also been provided in this thesis.

6.3 Future Work

The designed model is an initial step towards the development of the decentralised transactive energy systems. Currently, the model process only one energy transaction at a time. This simplified model design is intended to extend at a bigger level with enhancement of its features e.g. more functionalities will be added in the smart contract and mobile application, scalability of the software and hardware will be improved and more participants will be facilitated with the service. Moreover, continuous developments in the field of blockchain may also provide advanced features and tools that will be adapted to improve the model version.

Appendix A

Source code of Artifact 4

```
pragma solidity ^0.4.25;

contract EnergyTrade{
    struct Offer{
    uint32  ID;
    address seller;
    address buyer;
    string P2L_Hash;
    string L2P_Hash;
    uint32  energy;
    uint32 price;
    uint   timeOffered;
    uint   timePaidP2L;
    bool   picked;
    bool   P2L_Paid;
    bool   L2P_Paid;
    bool   delivered;

}
```

```
mapping(uint32 => Offer) public offers;
uint32 public offerID;


    function addOffer(uint32  energy, uint32  price) public {
        Offer storage newOffer = offers[offerID];
        newOffer.ID=offerID;
        newOffer.seller = msg.sender;
        newOffer.energy = energy;
        newOffer.price = price;
        newOffer.timeOffered = now;
        newOffer.picked = false;
        newOffer.P2L_Paid = false;
        newOffer.L2P_Paid = false;
        newOffer.delivered = false;
        offerID+=1;
    }

    function pickOffer(uint32 id) public {
        offers[id].picked = true;

    }

    function confirmP2L_Tx(uint32 id,string P2L_Hash) public {
        offers[id].P2L_Paid = true;
        offers[id].P2L_Hash = P2L_Hash;
        offers[id].buyer = msg.sender;
        offers[id].timePaidP2L= now;

    }
    function PoD(uint32 id) public{
        offers[id].delivered= true;
    }

    function confirmL2P_Tx(uint32 id,string L2P_Hash) public {
        offers[id].L2P_Paid = true;
        offers[id].L2P_Hash = L2P_Hash;
    }


}
```

Bibliography

[1] International Energy Agency. Renewables 2017. Technical report, International Energy Agency (IEA), 2017.

[2] Arshdeep Bahga and Vijay K Madisetti. Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications*, 9(10):533, 2016.

[3] Wouter Penard and Tim van Werkhoven. On the secure hash algorithm family. *Cryptography in Context*, pages 1–18, 2008.

[4] Barrie. Different types of blockchains. `https://businessdailybuzz.com/different-types-of-blockchains/`, May 2018.

[5] Hadelin de Ponteves SuperDataScience Team, Kirill Eremenko. Blockchain a-z^{TM}: Learn how to build your first blockchain, 2018.

[6] Fran Casino, Thomas K Dasaklis, and Constantinos Patsakis. A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics and Informatics*, 2018.

[7] Johnny Simon Joon Ian Wong. Photos: Inside one of the world's largest bitcoin mines. `https://qz.com/1055126/photos-china-has-one-of-worlds-largest-bitcoin-mines/`, August 2017.

[8] TheRealSteve. Bitcoin controlled supply. `https://en.bitcoin.it/wiki/Controlled_supply`, June 2015.

[9] Luis Ivan Cuende García Adán Sánchez de Pedro Crespo. Stampery blockchain timestamping architecture (bta). *CoRR*, October 2016.

[10] Ethereum. Gas costs from yellow paper – eip-150 revision (1e18248 - 2017-04-12). `https://wiki.learnblockchain.cn/OPCODE_Gas.pdf`, April 2017.

[11] Yang Lu. The blockchain: State-of-the-art and research challenges. *Journal of Industrial Information Integration*, 2019.

[12] Francisco Boshell Sean Ratka and Arina Anisie. Irena blockchain innovation landscape brief. Technical report, International Renewable Energy Agency (IRENA), February 2019.

[13] Merlinda Andoni, Valentin Robu, David Flynn, Simone Abram, Dale Geach, David Jenkins, Peter McCallum, and Andrew Peacock. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.*, 100(October 2018):143–174, 2019.

[14] International Renewable Energy Agency (IRENA). A roadmap to 2050. Technical report, International Renewable Energy Agency (IRENA), April 2018.

[15] John Conti, Paul Holtberg, Jim Diefenderfer, Angelina LaRose, James T Turnure, and Lynn Westfall. International energy outlook 2016 with projections to 2040. Technical report, USDOE Energy Information Administration (EIA), Washington, DC (United States . . . , 2016.

[16] Robert H Lasseter. Microgrids. In *2002 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No. 02CH37309)*, volume 1, pages 305–308. IEEE, 2002.

[17] Gary Giuliani Raimondo Geneiatakis Dimitrios Neisse Ricardo Nai-Fovino Igor Kounelis, Ioannis Steri. Fostering consumers' energy market through smart contracts. *Energy and Sustainability in Small Developing Economies, ES2DE 2017 - Proceedings*, 2017.

[18] Pierluigi Siano, Giuseppe De Marco, Alejandro Rolan, and Vincenzo Loia. A Survey and Evaluation of the Potentials of Distributed Ledger Technology for Peer-to-Peer Transactive Energy Exchanges in Local Energy Markets. *IEEE Syst. J.*, pages 1–13, 2019.

[19] Nakamoto Satoshi and Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic cash system. *Bitcoin*, page 9, 2008.

[20] F. Wessling, C. Ehmke, M. Hesenius, and V. Gruhn. How much blockchain do you need? towards a concept for building hybrid dapp architectures. In *2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, pages 44–47, May 2018.

[21] Manisa Pipattanasomporn, Murat Kuzlu, and Saifur Rahman. A Blockchain-based Platform for Exchange of Solar Energy: Laboratory-scale Implementation. *Proc. Conf. Ind. Commer. Use Energy, ICUE*, 2018-Octob(October):1–9, 2019.

[22] Zhou Su, Yuntao Wang, Qichao Xu, Minrui Fei, Yu Chu Tian, and Ning Zhang. A Secure Charging Scheme for Electric Vehicles with Smart Communities in Energy Blockchain. *IEEE Internet Things J.*, PP(c):1, 2018.

[23] Sana Noor, Wentao Yang, Miao Guo, Koen H. van Dam, and Xiaonan Wang. Energy Demand Side Management within micro-grid networks enhanced by blockchain. *Appl. Energy*, 228(June):1385–1398, 2018.

[24] Esther Mengelkamp, Johannes Gärttner, Kerstin Rock, Scott Kessler, Lawrence Orsini, and Christof Weinhardt. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. *Appl. Energy*, 210:870–880, 2018.

[25] Power Ledger. Power ledger white paper. `https://powerledger.io/`, 2018.

[26] Verv. Verv vlux whitepaper – the evolution of energy. `https://verv.energy/`, 2018.

[27] Alex Miller et al. Welcome to the future of energy. *Grid+, http://gridplus.io/whitepaper*, 2018.

[28] W. Liu, J. Zhan, and C. Y. Chung. A novel transactive energy control mechanism for collaborative networked microgrids. *IEEE Transactions on Power Systems*, 34(3):2048–2060, May 2019.

[29] Europäische Union. Directive 2009/28/ec of the european parliament and of the council of 23 april 2009 on the promotion of the use of energy from renewable sources and amending and subsequently repealing directives 2001/77/ec and 2003/30/ec. *Official Journal of the European Union*, 5:2009, 2009.

[30] David Livingston, Varun Sivaram, Madison Freeman, and F Maximilian. Applying block chain technology to electric power systems. Technical report, Discussion Paper. Council on Foreign Relations, 2018.

[31] J.A. Peças Lopes, N. Hatziargyriou, J. Mutale, P. Djapic, and N. Jenkins. Integrating distributed generation into electric power systems: A review of drivers, challenges and opportunities. *Electric Power Systems Research*, 77(9):1189 – 1203, 2007. Distributed Generation.

[32] Tomas Kåberger. Progress of renewable electricity replacing fossil fuels. *Global Energy Interconnection*, 1(1):48 – 52, 2018.

[33] Lea Diestelmeier. Changing power: Shifting the role of electricity consumers with blockchain technology–policy implications for eu electricity law. *Energy policy*, 128:189–196, 2019.

[34] Hendrik Kondziella and Thomas Bruckner. Flexibility requirements of renewable energy based electricity systems–a review of research results and methodologies. *Renewable and Sustainable Energy Reviews*, 53:10–22, 2016.

[35] Imke Lammers and Lea Diestelmeier. Experimenting with law and governance for decentralized electricity systems: adjusting regulation to reality? *Sustainability*, 9(2):212, 2017.

[36] Wenye Wang and Zhuo Lu. Cyber security in the smart grid: Survey and challenges. *Computer networks*, 57(5):1344–1371, 2013.

[37] Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang. Smart grid—the new and improved power grid: A survey. *IEEE communications surveys & tutorials*, 14(4):944–980, 2011.

[38] Keke Gai, Yulu Wu, Liehuang Zhu, Meikang Qiu, and Meng Shen. Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Transactions on Industrial Informatics*, 2019.

[39] Michael Mylrea and Sri Nikhil Gupta Gourisetti. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In *2017 Resilience Week (RWS)*, pages 18–23. IEEE, 2017.

[40] Stuart Haber and W. Scott Stornetta. How to time-stamp a digital document. In Alfred J. Menezes and Scott A. Vanstone, editors, *Advances in Cryptology-CRYPTO' 90*, pages 437–455, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.

[41] Satoshi Nakamoto. Original bitcoin sourcecode. `https://github.com/trottier/originalbitcoin`, 2013.

[42] Wikipedia. Blockchain. `https://en.wikipedia.org/wiki/Blockchain`, August 2019.

[43] Cryptoeconomics. The blockchain economy: A beginner's guide to institutional cryptoeconomics. `https://medium.com/cryptoeconomics-australia/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4`, September 2017.

[44] The Institute of Public Affairs. The blockchain revolution. `https://ipa.org.au/ipa-review-articles/the-blockchain-revolution`, December 2017.

[45] Vitalik Buterin. The meaning of decentralization. `https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274`, February 2017.

[46] Peter Smith Ben Reeves, Nicolas Cary. Blockchain. `https://www.blockchain.com/`, August 2011.

[47] Even Scharning. Unix time. `https://time.is/Unix_time_now`, 2009.

[48] Matthew Tan. Etherscan. `https://etherscan.io/chart/difficulty`, 2015.

[49] Bitcoin.com. How to setup a bitcoin asic miner. `https://www.bitcoin.com/get-started/how-to-setup-a-bitcoin-asic-miner-and-what-they-are`, 2019.

[50] Bitcoin Wiki. The mining ecosystem. `https://en.bitcoin.it/wiki/Mining#The_mining_ecosystem`, June 2018.

[51] Jordan Tuwiner. Bitcoin mining pools. `https://www.buybitcoinworldwide.com/mining/pools/`, January 2019.

[52] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[53] Nutthakorn Chalaemwongwan and Werasak Kurutach. State of the art and challenges facing consensus protocols on blockchain. In *2018 International Conference on Information Networking (ICOIN)*, pages 957–962. IEEE, 2018.

[54] Peercoin Foundation. peercoin: Pioneer of proof of stake. `https://peercon.net/`, 2019.

[55] Wilton Thornburg. What is ethereum? — the ultimate beginners' guide. `https://coincentral.com/what-is-ethereum-the-ultimate-beginners-guide/`, September 2018.

[56] Parity Technologies. Proof-of-authority chains - wiki. `https://wiki.parity.io/Proof-of-Authority-Chains`.

[57] Vitalik Buterin. On public and private blockchains. `https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/`, August 2015.

[58] Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, and Chen Qijun. A review on consensus algorithm of blockchain. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 2567–2572. IEEE, 2017.

[59] Alex Hughes, Andrew Park, Jan Kietzmann, and Chris Archer-Brown. Beyond bitcoin: What blockchain and distributed ledger technologies mean for firms. *Business Horizons*, 62(3):273–281, 2019.

[60] H. Treiblmaier and R. Beck. *Business Transformation through Blockchain*. Springer International Publishing, 2018.

[61] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 3:37, 2014.

[62] X. Wu and W. Sun. *Blockchain Quick Start Guide: A beginner's guide to developing enterprise-grade decentralized applications*. Packt Publishing, 2018.

[63] Ned Scott. steemit. `https://steemit.com/`, January 2016.

[64] John Quinn Shawn Wilkinson Tome Boshevski James Prestwich, Jim Lowry. storj. `https://storj.io/`, 2014.

[65] State of the DApps. What's a dapp. `https://www.stateofthedapps.com/whats-a-dapp`, 2019.

[66] Vitalik Buterin. Daos, dacs, das and more: An incomplete terminology guide. `https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/`, May 2014.

[67] Matthew Leising. The ether thief. https://www.bloomberg.com/features/2017-the-ether-thief/, June 2017.

[68] Antonio Madeira. https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/, March 2019.

[69] John Light. The differences between a hard fork, a soft fork, and a chain split, and what they mean for the future of bitcoin. https://medium.com/@lightcoin/the-differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9, September 2017.

[70] National Institute of Standards and Technology (NIST). Post-quantum cryptography. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography, January 2019.

[71] Weichao Gao, William G Hatcher, and Wei Yu. A survey of blockchain: techniques, applications, and challenges. In *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–11. IEEE, 2018.

[72] CHEN Sijie and LIU Chen-Ching. From demand response to transactive energy: state of the art. *Journal of Modern Power Systems and Clean Energy*, 5(1):10–19, 2017.

[73] RB Melton. Gridwise transactive energy framework version 1. grid-714 wise archit. council, richland, wa. Technical report, USA, Tech. Rep. PNNL-22946, 715: 716, 2015.

[74] Ariana Ramos, Cedric De Jonghe, Virginia Gómez, and Ronnie Belmans. Realizing the smart grid's potential: Defining local markets for flexibility. *Utilities Policy*, 40:26–35, 2016.

[75] Aysajan Abidin, Abdelrahaman Aly, Sara Cleemput, and Mustafa A Mustafa. Secure and privacy-friendly local electricity trading and billing in smart grid. *arXiv preprint arXiv:1801.08354*, 2018.

[76] Marcelo Sandoval and Santiago Grijalva. Future grid business model innovation: distributed energy resources services platform for renewable energy integration. In *2015 Asia-Pacific Conference on Computer Aided System Engineering*, pages 72–77. IEEE, 2015.

[77] Arman Kiani Bejestani, Anuradha Annaswamy, and Tariq Samad. A hierarchical transactive control architecture for renewables integration in smart grids: Analytical modeling and stability. *IEEE Transactions on Smart Grid*, 5(4):2054–2065, 2014.

[78] Zhaoxi Liu, Qiuwei Wu, Shaojun Huang, and Haoran Zhao. Transactive energy: A review of state of the art and implementation. In *2017 IEEE Manchester PowerTech*, pages 1–6. IEEE, 2017.

[79] Stefanie Kesting, Frits Bliek, and FP Sioshansi. From consumer to prosumer: Netherland's powermatching city shows the way. In *Energy Efficiency*, pages 355–373. Academic Press, 2013.

[80] EXERGY. Electric power technical whitepaper: Building a robust value mechanism to facilitate transactive energy. https://exergy.energy/wp-content/uploads/2017/12/Exergy-Whitepaper-v8.pdf, December 2017.

[81] Stefan Kapferer. Blockchain in the energy sector the potential for energy providers. https://www.bdew.de/media/documents/Studie-Blockchain-englische-Fassung-Dez.2018.pdf, May 2018.

[82] Pierre Pinson, Thomas Baroche, Fabio Moret, Tiago Sousa, Etienne Sorin, and Shi You. The emergence of consumer-centric electricity markets. *Distribution & Utilization*, 34(12):27–31, 2017.

[83] Indigo Advisory Group. Blockchain in the energy and utilities (use cases ,vendor activity ,market analysis). https://www.indigoadvisorygroup.com/blockchain, February 2017.

[84] Biljana L Risteska Stojkoska and Kire V Trivodaliev. A review of internet of things for smart home: Challenges and solutions. *Journal of Cleaner Production*, 140:1454–1464, 2017.

[85] Manar Jaradat, Moath Jarrah, Abdelkader Bousselham, Yaser Jararweh, and Mahmoud Al-Ayyoub. The internet of energy: smart sensor networks and big data management for smart grid. *Procedia Computer Science*, 56:592–597, 2015.

[86] Gerard Bel. Pylon. https://pylon-network.org/, 2017.

[87] Asger Trier Bing. Mpayg- democratizing access to energy. http://www.mpayg.com/, 2013.

[88] Weisong Shi, Jie Cao, Quan Zhang, Youhuizi Li, and Lanyu Xu. Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 3(5):637–646, 2016.

[89] Wei Yu, Fan Liang, Xiaofei He, William Grant Hatcher, Chao Lu, Jie Lin, and Xinyu Yang. A survey on the edge computing for the internet of things. *IEEE access*, 6:6900–6919, 2017.

[90] Fan Liang, Wei Yu, Dou An, Qingyu Yang, Xinwen Fu, and Wei Zhao. A survey on big data market: Pricing, trading and protection. *IEEE Access*, 6:15132–15154, 2018.

[91] Energy Web Foundation. The energy web. https://www.energyweb.org/reports/the-energy-web-chain/, 2017.

[92] Hyperledger. An introduction to hyperledger. https://www.hyperledger.org/, August 2018.

[93] Wayes Tushar, Chau Yuen, Hamed Mohsenian-Rad, Tapan Saha, H Vincent Poor, and Kristin L Wood. Transforming energy networks via peer to peer energy trading: Potential of game theoretic approaches. *arXiv preprint arXiv:1804.00962*, 2018.